



عمادة الدراسات العليا

جامعة القدس

الذِّكَاؤُ العاطِفيُّ وعَلاقَتُهُ بِمُمارَسةِ جَرائِمِ الابتِزازِ الإِلِكْترُونيِّ لَدَى عَيِّنَةٍ مِنَ
الضَّحَايا فِي الضَّفَّةِ العَرَبِيَّةِ

نورهان هاني إسماعيل عابدين

رسالة ماجستير

القدس - فلسطين

1441هـ / 2020م

الدَّكَاؤُ العَاطِفِيُّ وَعِلَاقَتُهُ بِمُمَارَسَةِ جَرَائِمِ الإِلِكْتَرُونِيِّ لَدَى عَيِّنَةٍ مِّنَ
الضَّحَايَا فِي الضَّفَّةِ الغَرِبِيَّةِ

إعداد:

نورهان هاني إسماعيل عابدين

بكالوريوس خدمة اجتماعية - جامعة القدس المفتوحة بيت لحم - فلسطين

المُشرف: د. وفاء الخَطِيب

قُدِّمَت هذه الدَّرَاسة استكمالاً لمتطلبات الحصول على درجة الماجستير في
الخدمة الاجتماعية، كلية الدراسات العليا/ جامعة القدس

1441هـ / 2020م



جامعة القدس

عمادة الدراسات العليا

برنامج ماجستير الخدمة الاجتماعية

إجازة الرسالة

الدِّكَاؤُ العَاطِفِيُّ وَعَلاقتُهُ بِمُمارِسةِ جَرائِمِ الِابْتِزازِ الإِلكِترُونِيِّ لَدَى عَيِّنَةٍ مِنَ الضَّحَايا

في الصَّفَّةِ العَرَبِيَّةِ

اسم الطالبة : نورهان هاني إسماعيل عابدين

الرقم الجامعي: 21510046

المشرف: د. وفاء الخطيب

تُوقِشت هذه الرسالة وأُجيزت بتاريخ: 2020/ 01/11 من لجنة المناقشة التالية أسماؤهم وتواقيعاتهم:

التوقيع:
التوقيع:
التوقيع:

1. رئيس لجنة المناقشة: د. وفاء الخطيب

2. المُمتحن الداخلي: د. علا حسين

3. المُمتحن الخارجي: د. عصام الأطرش

القدس - فلسطين

1441هـ / 2020م

الإهداء

أشكر الله - سبحانه تعالى - على ما أعطاني من النعم والعلم، وأعانني على طاعته...

إلى شفيعنا يوم الدين نبينا الكريم محمد صلى الله عليه و سلم

إلى أستاذتنا الأفاضل جميعهم الذين حملوا أقدس رسالة في الحياة، ومهدّوا لنا طريق العلم والمعرفة...

إلى من رباني وعلمني وأفنى عمره في تربيّتنا إلى قدوتي وسندي، (أبي الغالي)...

إلى مَنْ كانت الجنة تحت أقدامها إلى أحنَّ مَنْ في الوجود (أمي الحنونة)...

إلى رفيق دربي وزوجي الغالي (لؤي) ...

إلى ابنتي الغالية ونعمتي من الله (لارين)...

إلى النور الذي يبصرني الطريق، أخواتي وإخوتي...

إلى شهدائنا الأبرار وأسرانا اليواسل...

إلى الجنود المجاهدين في الجامعة: الدكتورة رولا هردل، والأستاذ وجدي حمائل

الباحثة:

نورهان عابدين

إقرار :

أقرّ أنا مُعدّة هذه الرسالة بأنّها قُدمت لجامعة القدس، لنيل درجة الماجستير، وأنها نتيجة أبحاثي الخاصة، باستثناء ما تمّت الإشارة إليه حيثما ورد، وأنّ هذه الدّراسة أو أي جزء منها لم يُقدّم لنيل درجة عليا لأية جامعة أو معهد آخر.

التوقيع:.....

الاسم: نورهان هاني إسماعيل عابدين

التاريخ: 2020/01/ 11

الشكر والتقدير

قال عليه الصلاة: (مَنْ لَا يَشْكُرُ النَّاسَ لَا يَشْكُرُهُ اللَّهُ)

الحمد لله رب العالمين والصلاة والسلام على سيد المرسلين محمد "عليه الصلاة والسلام".

لقد مَنْ الله عليّ بأن أتممت رسالة الماجستير، وأتقدم بجزيل الشكر والامتنان إلى مَنْ كان لهم الفضل بعد الله - سبحانه وتعالى- في إنجاز هذه الرسالة.

إلى مَنْ يُقدِّم رسالة سامية وعلماء وعطاء دون مقابل إلى جميع الأساتذة الكرام.

أتقدم بالشكر الجزيل إلى مشرفتي ومعلمتي الدكتورة وفاء سامح الخطيب على الإشراف والمساعدة في إتمام رسالتي المتواضعة حيث كان لجهدا عظيم الأثر في إخراج هذه الرسالة.

كما أتقدم بالشكر لأعضاء لجنة المناقشة الكرام، والمكونة من الممتحن الداخلي الدكتورة علا حسين، والممتحن الخارجي الدكتور عصام الأطرش الذين تفضلوا بقبول مناقشة هذه الرسالة، وإثرائها بأرائهم القيمة.

وكذلك أتقدم بالشكر والتقدير إلى وحدتي الجرائم الإلكترونية في جهاز الشرطة الفلسطينية والنيابة العامة، ووحدة حماية الاسرة في الشرطة الفلسطينية الممثلين في الدكتور أحمد براك، العقيد وفاء معمر، العقيد جهاد عبد الكريم، العقيد سامر المصري، المقدم باسل خريوش، الملازم أول سونيا عزاب، الأستاذ علاء التميمي، الاستاذة نسرین رشموي، كما اتقدم بالشكر الى كل من تقدم بتعبئة الاستبيان فلكم مني جميعاً عبارات الشكر والتقدير على تعاونكم.

قائمة المحتويات:

أ.....	إقرار :
ب.....	الشكر والتقدير
ج.....	قائمة المحتويات:
ز.....	قائمة الأشكال والجداول:
ك.....	الملخص:
م.....	Abstract:
1.....	الفصل الأول: الإطار العام للدراسة
1.1.....	1.1 مقدمة:.....
2.1.....	2.1 مشكلة الدراسة:
3.1.....	3.1 أهمية الدراسة:
4.1.....	4.1 أهداف الدراسة:
5.1.....	5.1 أسئلة الدراسة وفرضياتها:.....
6.1.....	6.1 حدود الدراسة:.....
8.....	الفصل الثاني: الإطار النظريّ والدراسات السابقة ذات العلاقة
8.....	1.1 الذكاء العاطفيّ:.....
8.....	1.1.2 مقدمة:.....
9.....	2.12 مفهوم الذكاء العاطفيّ:
11.....	3.1.2 التطور التاريخيّ لمفهوم الذكاء العاطفيّ ونشأته في علم النفس:
14.....	4.1.2 أهمية الذكاء العاطفيّ في بعض مجالات العلوم العلمية:
15.....	5.1.2 مكونات الذكاء العاطفيّ:.....
16.....	6.1.2 سمات الأشخاص الأذكياء عاطفياً:.....
17.....	7.1.2 مقاييس الذكاء العاطفيّ:

21	8.1.2 النظريات المفسرة للذكاء العاطفيّ:
24	2.2 جرائم الابتزاز الإلكترونيّ:
24	1.2.2 مقدمة:
25	2.2.2 مفهوم جرائم الابتزاز الإلكترونيّ:
27	3.2.2 التطور التاريخي لجرائم الابتزاز الإلكترونيّ:
30	4.2.2 أنواع جرائم الابتزاز الإلكترونيّ:
33	5.2.2 أركان جرائم الابتزاز الإلكترونيّ:
34	6.2.2 أسباب ارتكاب جرائم الابتزاز الإلكترونيّ:
35	7.2.2 خصائص جرائم الابتزاز الإلكترونيّ:
38	8.2.2 آثار جرائم الابتزاز الإلكترونيّ:
39	9.2.2 سمات وصفات الضحايا والجناة في جرائم الابتزاز الإلكترونيّ:
41	10.2.2 واقع الجرائم الإلكترونية في فلسطين:
47	11.2.2 أنواع الجرائم الإلكترونية في فلسطين:
	12.2.2 الصعوبات التي تواجه أصحاب الاختصاص في مكافحة جرائم الابتزاز الإلكترونيّ في فلسطين وطرق مكافحتها:
48	
50	13.2.2 الجهود المبذولة لمكافحة الجرائم الإلكترونية في العالم ودولة فلسطين المحتلة:
54	3.2 مواقع التواصل الاجتماعيّ:
54	1.3.2 مقدمة:
56	2.3.2 مفهوم مواقع التواصل الاجتماعيّ:
56	3.3.2 أنواع مواقع التواصل الاجتماعيّ ومميزاتها:
58	4.3.2 الاستخدامات الإيجابية والسلبية لمواقع التواصل الاجتماعيّ:
60	5.3.2 النظريات المفسرة لجرائم الابتزاز الإلكترونيّ:
65	4.2 الدراسات السابقة وذات العلاقة:
74	3.4.2 التعقيب على الدراسات السابقة:

76 الفصل الثالث: الطريقة والإجراءات 76

76 3 . 1 منهج الدراسة: 76

76 3.2 مجتمع الدراسة: 76

77 3 . 3 عينة الدراسة: 77

77 3 . 4 وصف متغيرات أفراد العينة: 77

78 3.5 أداة الدراسة: 78

79 3.5.1 صدق الأداة: 79

81 3.5.2 ثبات أداة الدراسة: 81

82 3 . 6 إجراءات الدراسة: 82

82 3 . 7 المعالجة الإحصائية: 82

83 الفصل الرابع: نتائج الدراسة 83

83 4 . 1 مقدمة: 83

84 4 . 2 نتائج أسئلة الدراسة: 84

84 4.2.1 النتائج المتعلقة بالسؤال الأول: 84

86 4.2.2 النتائج المتعلقة بالسؤال الرئيسي الثاني: 86

105 4.3 نتائج المقابلات: 105

111 الفصل الخامس: مناقشة النتائج والتوصيات 111

111 5.1 مناقشة نتائج أسئلة وفرضيات الاستبانة: 111

111 مناقشة النتائج المتعلقة بالسؤال الأول: 111

115 مناقشة نتائج السؤال الثاني: 115

115 مناقشة نتائج السؤال الفرعي الأول: 115

117 مناقشة نتائج السؤال الفرعي الثاني: 117

117 ما الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني 117

120 مناقشة نتائج السؤال الفرعي الثالث: 120

122 مناقشة نتائج السؤال الفرعي الرابع:
125 مناقشة نتائج السؤال الثالث:
126 مناقشة نتائج السؤال الرابع:
132 2.5 مناقشة النتائج المتعلقة بالمقابلات:
143 3.5 ملخص النتائج :
145 4.5 التوصيات:
147 قائمة المصادر والمراجع
164 قائمة الملاحق

قائمة الأشكال والجدول:

رقم الجدول	الموضوع	الصفحة
1.3	توزيع أفراد عينة الدراسة الذين تم توزيع الاستبانة عليهم حسب متغيرات الدراسة	77
2.3	نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات مستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية	79
3.3	نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية	80
4.3	نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني من وجهة نظر الضحايا.	80
5.3	نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع ضحايا جرائم الابتزاز الإلكتروني الضفة الغربية	80
6.3	نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.	81
7.3	نتائج معامل الثبات للمجالات	81
1.4	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.	84
2.4	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لواقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية	86
3.4	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني	87

89	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني	4.4
91	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع ضحايا جرائم الابتزاز الإلكتروني	5.4
93	المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا	6.4
95	معامل ارتباط بيرسون والدلالة الاحصائية للعلاقة بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا	7.4
96	نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني حسب متغير الجنس	8.4
96	المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي	9.4
97	نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي	10.4
97	نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير المستوى التعليمي	11.4
98	المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن	12.4
98	نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن	13.4
99	المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر	14.4
100	نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر	15.4
100	نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني	16.4

	حسب متغير الوظيفة	
101	المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل	17.4
102	نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل	18.4
102	نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني حسب متغير الحالة الاجتماعية	19.4
103	المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي	20.4
104	نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي	21.4
104	نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير معدل الاستخدام لمواقع التواصل الاجتماعي	22.4

قائمة الملاحق:

الصفحة	الموضوع	الملحق
165	الاستبانة في صورتها الأولى	ملحق (1)
175	الاستبانة في صورتها النهائية	ملحق (2)
Error! Bookmark not defined.	قائمة بأسماء محكمي الاستبانة	ملحق (3)
187	تسهيل المهمة	ملحق (4)
189	نتائج المقابلات	ملحق (5)
214	قانون رقم (10) لسنة (2017)	ملحق (6)
236	قانون رقم (10) لسنة 2018	ملحق (7)
255	مذكرة قانونية حول القرار بقانون رقم (10) لسنة 2018 فيما يخص الجرائم الإلكترونية	ملحق (8)

المخلص:

هدفت الدراسة التعرف إلى الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية، استخدمت الدراسة المنهج الوصفي بشقيه: الكمي من خلال استخدام أداة الاستبانة التي صممت خصيصا من أجل الحصول على البيانات من الضحايا، والكيفي من خلال المقابلة إذ صم لها استبانة تُسمى استبانة المقابلة من أجل الحصول على البيانات من العاملين في وحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في كل من النيابة العامة والشرطة الفلسطينية، وتكون مجتمع الدراسة من (208) ضحية لجرائم الابتزاز الإلكتروني حسب إحصائيات النيابة العامة والشرطة الفلسطينية، في حين بلغت عينة الدراسة (73) ضحية من وحدة الجرائم الإلكترونية، ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة تم اختيارهم بطريقة قصدية، إضافة لذلك تم عمل مقابلة مع (5) من أفراد عاملين في وحدتي الجرائم الإلكترونية وحماية الأسرة في جهاز الشرطة الفلسطينية والنيابة الجرائم الإلكترونية في النيابة العامة.

توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها أن مستوى الذكاء العاطفي يؤثر على زيادة ممارسة جرائم الابتزاز الإلكتروني، فمستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني جاء بدرجة متوسطة وبلغ المتوسط الحسابي للدرجة الكلية (3.39)، في حين توصلت الدراسة كذلك إلى أن الابتزاز المالي والجنسي والتشهير من أكثر أنواع جرائم الابتزاز الإلكتروني انتشاراً، كما تبين أن أهم الصعوبات التي تحد من عمل وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة تتمثل في ضعف مستوى الإمكانيات المادية، وعدم وجود أجهزة حديثة، وطواقم مدربة ومؤهلة للتصدي للجناة في هذه الجرائم تحديداً في الحالات التي يتميز بها مرتكب الجرائم الإلكترونية بمستوى مرتفع من الذكاء العاطفي في المقابل أشارت النتائج إلى أن أهم الإجراءات المتبعة من "وحدة الجرائم الإلكترونية، ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة" في التعامل مع جرائم الابتزاز الإلكتروني أنها تتم بسرية تامة، كما أشارت النتائج إلى أن الاختلاط بأصدقاء السوء من أهم الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني، وأن العلاقات العاطفية تُعد من أهم الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني، إضافة أنها أشارت إلى أن أهم الآثار التي تنتج عن الابتزاز الإلكتروني هي

التفكك الأسري، وانتشار الانحراف بين الضحايا والمبتزين، بينما أشارت نتائج المقابلات إلى أنّ هناك حالات تتعرض للصدمة النفسية، ويمكن أن تؤدي في بعض الحالات إلى الموت، وأشارت النتائج أيضا إلى أنّه لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا، كذلك أشارت النتائج إلى عدم وجود فروق دالة إحصائية تبعا لمتغيرات الدراسة (الجنس، المستوى التعليمي، مكان السكن، العمر، الوظيفة، مستوى الدخل، الحالة الاجتماعية، معدل استخدام مواقع التواصل الاجتماعي).

في حين توصلت الدراسة إلى مجموعة من التوصيات كان من أهمها العمل على رفع مستوى الوعي الوقائي لدى جميع أفراد المجتمع حول جرائم الابتزاز الإلكتروني، ذلك من خلال البرامج التلفزيونية والنشرات الإرشادية من قبل الشرطة الفلسطينية ليكون لدى المواطن الوعي الكافي بوجود مثل هذه الجرائم في المجتمع ورفع مستوى الثقة بالنيابة العامة وجهاز القضاء الفلسطيني من خلال تطبيق القانون الخاص بالجرائم الإلكترونية المعدل ونشر جلسات المحاكمة لأفراد المجتمع من خلال وسائل الإعلام المختلفة لتكون رادعا للجناة واكتساب ثقة المواطنين، كذلك ضرورة اهتمام الأفراد المستخدمين للشبكة العنكبوتية بعمل فحص دوري لأجهزتهم، وتنشيط برامج الحماية المرخصة من قبل شركات الإنترنت الفلسطينية، وعدم استخدام الحسابات الخاصة بهم في الأماكن العامة غير الموثوقة حتى لا يتعرضوا لجرائم الابتزاز الإلكتروني، إضافة إلى تخصيص ميزانية لمكافحة الجرائم الإلكترونية وتدريب العاملين في هذا المجال على أحدث التقنيات لمحاولة التقليل والسيطرة على هذه الجرائم.

الكلمات مفتاحية: الذكاء، الذكاء العاطفي، الابتزاز، الابتزاز الإلكتروني، الجريمة، الضحايا.

The Emotional intelligence and its relationship to the practice of cyber blackmail in a sample of victims in the West Bank

Prepared by: Nourhan Hani Ismael Abdeen

Supervisor: Dr.Wafaa Khateeb

Abstract:

The study aimed at identifying the emotional intelligence and its relationship to the practice of cyber blackmail in a sample of victims in the West Bank. The study used the quantitative descriptive approach through the use of a questionnaire tool designed specifically for obtaining data from the victims. She also used qualitative descriptive approach via an interview In order to obtain data from the staff of the Family Protection Unit and the E-Crime Prosecution in both the Palestinian Police and Public Prosecution. The study population consists of (208) victims of cyber blackmail crimes according to the prosecution statistics. The study sample included (73) victims from the cybercrime unit, the family protection unit in the Palestinian police and the cybercrime prosecution in the public prosecution were selected in an intentional manner. In addition, an interview was conducted with (5) individuals who works in the Electronic crime and family protection units in the Palestinian police and public prosecution.

The study reached a set of results, the most important of which is that the level of emotional intelligence affects the increase in the practice of cyber blackmail crimes. The level of emotional intelligence among victims of cyber blackmail crimes was medium and the average of the total score (3.39). However, the study also found that financial and sexual extortion and defamation are among the most common types of cyber blackmail. The study also found the main difficulties that limit the work of the Cybercrime Unit and the Family Protection Unit in the are the limitation of the financial resources. In addition, there is a lack of modern equipment and trained qualified staff to deal with the perpetrators of these crimes, especially in cases where the perpetrator of a cybercrime is characterized by a high level of emotional intelligence. On the other hand, the results indicated that the procedures followed by the "Cybercrime Unit, the Family Protection Unit in the Palestinian Police Authority and the Cybercrime Prosecution in the Public Prosecution" in dealing with cyber blackmail crimes are completely confidential. The results also indicated that bad friends are one of the most important reasons that lead to cyber blackmail crimes, and that emotional relationships are one of the most important ways used to inflict victims of cyber blackmail crimes. in addition, the study pointed out that the most important effects resulting from cyber blackmail are family disintegration, The spread of deviation between

victims and blackmailers, while the results of the interviews indicated that there are cases of psychological trauma and can lead in some cases to death. The results also indicated that there is no statistically significant relationship at the level of significance ($\alpha \leq 0.05$) between the level of intelligence and the practice of crimes of electronic blackmail for the victims. Also, there are no statistically significant differences according to study variables (sex, educational level, place Housing, Age, employment, income level, marital status, social media usage rate).

The study reached a set of recommendations, the most important of which is to raise the level of preventive awareness among all members of the society about the crimes of electronic blackmail, through television programs and bulletins by the Palestinian police. This will lead to a sufficient awareness of the existence of such crimes in the community and it will raise the level of trust in the public prosecution and the Palestinian judiciary. This will be achieved through the application of the amended law on cybercrime and the publication of trial sessions for members of the community through the various media to be a deterrent to the perpetrators and gain the trust of citizens. Also the need for the individuals who use the network Spyware to check their computers, install security programs licensed by Palestinian Internet companies, and not use their accounts in public places that are not trusted so as not to be subjected to cyber blackmail. Finally , to allocate a budget to combat cybercrime and train the workers in this field to try to minimize and control these crimes.

Key words: Intelligence, Emotional intelligence, Blackmail, cyber blackmail, Crime, Victims.

الفصل الأول

الاطار العام للدراسة

1.1 مقدمة:

منذ أوائل هذا القرن بدا العالم يشهد قدرا كبيرا من التغيرات على الصعيد الاجتماعي والأمني والاقتصادي والتكنولوجي، إذ تميزت هذه الحقبة بوتيرة التطورات السريعة المستمرة اللامتناهية من التقنيات والتكنولوجيا، لتحمل في طياتها العديد من التبعيات الإيجابية والسلبية، حيث تتمثل السلبية في عدم معرفة الفرد لذاته وللآخرين، الأمر الذي أدى إلى عدم قدرته على مواكبة الواقع الذي يعيشه، بسبب عدم ملائمة نمط الحياة العصرية، والمتطلبات الطارئة التي نتجت عن الحداثة المستمرة سواء على الصعيد التكنولوجي أو الاجتماعي، حيث لا تنطبق هذه المتطلبات الجديدة مع حاجة الأفراد إلى الاختلاء مع الذات والتأمل في أحوالها واحتياجاتها الحقيقية، مما قد يؤثر على مستوى الذكاء العاطفي لديه ومن الممكن أن يزيد من فرص تعرضه لجرائم الابتزاز الإلكتروني (سلامي، 2016).

وبتغير طريقة التواصل بين الأفراد بسبب التطور التكنولوجي واستخدام الهاتف المحمول وأجهزة الحاسوب من خلال مواقع التواصل الاجتماعي بشكل غير مباشر، تعرض بعض الأفراد في المجتمع إلى التأثير السلبي من هذا النوع من التواصل بسبب اعتمادهم الكلي عليها في التواصل مع الغير، مما أثر على مستوى الذكاء العاطفي لديهم الذي يتكون من خلال الاتصال والتواصل مع الآخرين، إضافة إلى ذلك عدم إدراكهم لكيفية استخدام هذه المواقع بأمان، لسرعة انتشارها بين الناس واعتمادها للتواصل لدى العديد من الأفراد في المجتمع بمختلف الشرائح العمرية، فلم يدركوا الكيفية الصحيحة

للتعامل معها، ممّا جعلهم أكثر عرضة للمخاطر بسبب استهتارهم واستخدامهم غير الواعي لها، هذه أحد سلبيات مواقع التواصل الاجتماعيّ، إضافة إلى أنّها تقود الفرد إلى التبعيّة النفسيّة والانفعاليّة بسبب اعتقاد البعض منهم أنّها توفر لهم فهمًا لذاتهم وللآخرين (الظاهري، 2017).

وفي السياق نفسه يمكن القول: إنّ أكثر ما تعرض له الأفراد من خلال هذا النوع من التواصل هو ما يخصّ توجه المبتزين للحصول على المال، فكونها أصبحت متوافرة لدى أغلب الأفراد في منازلهم جعل وقوع الأفراد كضحايا لجرائم الابتزاز الإلكترونيّ أسهل، وذلك لضعف مستويات الأمان المتوفرة سواء على مستوى هذه المواقع أو على مستوى الشبكة العنكبوتيّة بشكل عام، تحديدا وأنّ الشبكة العنكبوتيّة أصبحت حقًا من حقوق الإنسان لا يحق لأحد التدخل في الحدّ من استخدامها، هذا جميعه حدث بسبب عولمة حقوق الإنسان التي كان له دور في انتشار ممارسة الجرائم بأشكال وأنواع محددة، بالإضافة إلى وجود بعض الأشخاص ذوي الثقافات العدوانية وقلة وعي بعض مستخدمي الشبكة العنكبوتيّة وخطورة ما يدلون به من معلومات لأشخاص غير موثوق بهم، أو بتعرضهم للاحتيال ونهب المعلومات الخاصة، حيث يعدّ التعارف الطريق الأول للمبتز للإيقاع بضحاياه من خلال مواقع التواصل الاجتماعيّ مثل: (فيس بوك، توتير، وإنستغرام،...الخ)، إذ من الممكن أن يطلب الجاني من الضحية تصوير جسدها، أو تسجيل محادثة بالكاميرا، ويستخدمها الجاني فيما بعد من أجل ابتزاز الضحية، ممّا يعني انصياع بعض الضحايا لأوامر الجاني الذي قدموا له معلومات عن حياتهم الخاصة مقابل وعوده للضحية بالزواج أو بالمساعدة في الحياة العامة كالوصول على الوظيفة أو المساعدة بالدراسة وغيرها من الاحتياجات، بمعنى استغلال الضحية بمجموعة من المشاعر التي تفتقر إليها، إضافة إلى أنّه من الممكن استغلال الجاني للضحية التي تتسم بعدم ارتفاع مستوى الذكاء العاطفيّ لديها ورغبتها في الحصول على علاقة عاطفية تحلم بها، ممّا يعني تهديد أمن الفرد والمجتمع معاً، فالأمن نعمة من نعم الله - سبحانه وتعالى - على الأفراد، وقد ورد في القرآن الكريم في أكثر من موضع منها قوله سبحانه وتعالى: (وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَدًا آمِنًا وَارْزُقْ أَهْلَهُ مِنَ الشُّرَكَاتِ مَنْ آمَنَ مِنْهُمْ بِاللَّهِ وَالْيَوْمِ الْآخِرِ قَالَ وَمَنْ كَفَرَ فَأُمْتِعْهُ قَلِيلًا ثُمَّ أَضْطَرُّهُ إِلَىٰ عَذَابِ النَّارِ وَبِئْسَ الْمَصِيرُ) صدق الله العظيم (سورة البقرة، الآية 126).

على ضوء ما سبق تسعى الدراسة التعرف إلى الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية، حيث يتكون الذكاء العاطفي من العديد من المكونات لعل من أهمها: العواطف الأخلاقية، وحلّ المشكلات، والمهارات الاجتماعية، ومهارة التفكير، وسيتم توضيح علاقة تلك المكونات بواقع الضحية التي تتصف بارتفاع مستوى الذكاء العاطفي أو عدمه، وعلاقته بوقوعها كضحية لمرتكب جرائم الابتزاز الإلكتروني في فلسطين بشكل عام والضفة الغربية بشكل خاص.

2.1 مشكلة الدراسة:

أسهم التطور في المجال التقني والتكنولوجي في إيجاد أنواع جديدة من الجرائم التي لم تكن معروفة سابقاً، لعل من أهمها جرائم "الابتزاز الإلكتروني"، التي أسهم في انتشارها الاستخدام الخاطئ وغير الواعي للشبكة العنكبوتية (الإنترنت)، إضافة إلى عدم اتخاذ التدابير اللازمة للأمن والحماية، مما قد يؤدي إلى زيادة الجرائم الإلكترونية التي تتضمن جرائم الابتزاز الإلكتروني، هذا ما أشارت إليه إحصائيات (جهاز الشرطة الفلسطينية، 2019) بأنّ هناك ارتفاعاً في معدلات الجرائم الإلكترونية في فلسطين التي ظهرت بعد التطور التكنولوجي وانتشار خدمة الإنترنت، إذا شهد عام (2016) على سبيل المثال (1327) شكوى مقارنة في عام (2015) ليسجل (502) شكوى لتصبح النسبة بما يقارب الضعف، بينما في عام (2017) بلغت (2025) شكوى، مقارنة في العام (2018) إذ كانت (2568) شكوى، عند مقارنة عدد الشكاوي بنهاية كلّ عام نجد ازدياداً ملحوظاً في معدل الجرائم الإلكترونية. ووفق إفادة (الجهاز المركزي للإحصاء الفلسطيني و وزارة الاتصالات وتكنولوجيا المعلومات، 2017) في بيان مشترك "فإنّ هناك ارتفاعاً في نسبة الأفراد الذين يستخدمون الإنترنت في فلسطين حيث بلغت (57.4%) من كلا الجنسين، بناء على تقديرات الاتحاد الدولي للاتصالات مقارنة بما كانت عليه خلال العام (2014) بزيادة مقاديرها (6%)، وبلغ عدد مستخدمي مواقع التواصل الاجتماعي (1,250,00) مستخدم بمعدل ساعتين يومياً"، بالتالي من الممكن أن يزداد عدد ضحايا جرائم الابتزاز الإلكتروني نتيجة الاستخدام الخاطئ والمستهتر للشبكة العنكبوتية (الإنترنت) وضعف الرقابة الأسرية والدينية والأخلاقية للأبناء، مما قد يترتب عليها آثاراً على الصعيد (الاجتماعي، والأسري، والنفسي، والاقتصادي، والأمني، والأخلاقي).

ومن خلال متابعة الأخبار والتقارير التي تتعلق بجرائم الابتزاز الإلكتروني، وبعد الاطلاع على إحصائيات إدارة المباحث العامة في الشرطة الفلسطينية الممثلة بوحدة حماية الأسرة ووحدة الجرائم الإلكترونية ونيابة الجرائم الإلكترونية في النيابة العامة، يمكن القول: إنَّ هناك زيادة ملحوظة في معدل هذه الجرائم سنوياً، مع تنوع أساليب وأنماط تنفيذها، إذ من الممكن أن يكون من يستخدم الشبكة العنكبوتية (الإنترنت) ضحية أو جانٍ، بينما من الممكن أن تكون الضحية ذات دور كبير في زيادة معدل هذه الجرائم، خاصة فيما يتعلق في الذكاء العاطفي لديها وقدرتها على التعامل مع جرائم الابتزاز الإلكتروني ومساعدة الجاني باستغلال انخفاض مستوى الذكاء العاطفي لديها، وعدم إدراك كافة الأفراد للمخاطر التي تحملها التقنيات التكنولوجية الحديثة.

3.1 أهمية الدراسة:

تتبع أهمية الدراسة الحالية من أهمية الموضوع الذي تدرسه، تحديداً وإنَّ المجتمع الفلسطيني زاد استخدامه لمواقع التواصل الاجتماعيّ كغيره من المجتمعات الأخرى، كما وتتبع أهمية الدراسة من أهمية نظريتين: إحداهما علمية، وأخرى عملية تطبيقية، أما أهمية النظرية العلمية، فتمثل في:

- محاولة التعريف بالذكاء العاطفيّ ومعرفة علاقته بممارسة جرائم الابتزاز الإلكترونيّ لدى عيّنة من الضحايا في الضفة الغربية.
- تعتبر هذه الدراسة من الدراسات النادرة والقليلة في تلك المنطقة على حدِّ علم الباحثة، وبالتالي ستسهم في إغناء الأدبيات السابقة في هذا الموضوع، لتكون مصدرة علمياً للباحثين يستندون إليها في دراساتهم اللاحقة حسب تخصصاتهم المختلفة حينما يتعلق الأمر بالأمن المجتمعيّ.

في حين تتمثل الأهمية العملية التطبيقية في مجموعة الجهات التي سوف تستفيد من الدراسة على النحو الآتي:

- الأهل: من خلال التعرف على أهم أنواع الابتزاز الإلكترونيّ، وأكثرها انتشاراً لتوعية أبنائهم وحمايتهم من الوقوع في فخ جرائم الابتزاز الإلكترونيّ وتحولهم إلى ضحايا.

• **السياسيون ومنتخبو القرار:** من خلال النتائج التي تهدف لمعرفة الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني، فقد تساعدهم تلك النتائج بوضع سياسات وقوانين مناسبة للحدّ من تلك الظاهرة.

• **الجهات المختصة: (وحداتي الجرائم الإلكترونية في كلّ من النيابة العامة وجهاز الشرطة الفلسطينية، ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية):** تزويد المهتمين والمختصين في المؤسسات الأهلية والحكومية بنتائج الدراسة لوضع خطط استراتيجية توعوية ضرورية لمكافحة جرائم الابتزاز الإلكتروني والتقليل من ممارستها، ذلك لأنّ الأمن المجتمعيّ من أساسيات استقرار المجتمع وتوازنه.

4.1 أهداف الدراسة:

تكمّن أهداف الدراسة في هدفين رئيسان وأهداف أخرى فرعية، يتمثّل الهدف الرئيس الأول فيتمثّل في التعرف إلى الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية، أما الهدف الرئيس الثاني فيتمثّل في قياس كل من:

(1) مستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.
(2) واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية، أنبثق عن هذا الهدف الرئيس أهداف أخرى فرعية تتمثّل في التعرف إلى:

أ- الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.
ب- أهم الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني من وجهة نظر الضحايا.
ج- الإجراءات المتبعة من "وحداتي الجرائم الإلكترونية في النيابة العامة والشرطة الفلسطينية، ووحدة حماية الأسرة في الشرطة الفلسطينية" في التعامل مع ضحايا جرائم الابتزاز الإلكتروني.
د- الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.

(3) وجود علاقة في استجابة المبحوثين بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني.

(4) وجود فروق في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغيرات الدراسة (الجنس، العمر، المستوى التعليمي، مكان السكن، الوظيفة، الحالة الاجتماعية، معدل استخدامك لمواقع التواصل الاجتماعي في اليوم).

5.1 أسئلة الدراسة وفرضياتها:

تكمن أسئلة الدراسة في سؤال رئيس وأسئلة أخرى فرعية، فأما السؤال الرئيس فيتمثل في: "معلّقة الذكاء العاطفي بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية"، في حين تتمثل الأسئلة الفرعية في:

1. ما مستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية؟
2. ما واقع جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية؟ وسيتم الإجابة على هذا السؤال من خلال الأسئلة الفرعية الآتية:

أ- ما الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية؟

ب- ما الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني من وجهة نظر الضحايا؟

ج- ما الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة" في التعامل مع ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية؟

د- ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟

(1) هل توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة الباحثين

بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني؟

(2) هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة الباحثين

حول ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغيرات الدراسة (الجنس، العمر، المستوى التعليمي، مكان السكن، الوظيفة، الحالة الاجتماعية، معدل استخدامك لمواقع التواصل الاجتماعي في اليوم)؟، سوف يتم الإجابة على هذا السؤال من خلال الفرضيات الآتية:

• توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة الباحثين حول

ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير الجنس.

• توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة الباحثين حول

ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير المستوى التعليمي.

• توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة الباحثين حول

ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير مكان السكن.

- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الإبتزاز الإلكتروني تعزى لمتغير العمر.
- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الإبتزاز الإلكتروني تعزى لمتغير الوظيفة.
- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الإبتزاز الإلكتروني تعزى لمتغير مستوى الدخل.
- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة مبحوثين حول ممارسة جرائم الإبتزاز الإلكتروني تعزى لمتغير الحالة الاجتماعية.
- توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الإبتزاز الإلكتروني تعزى لمتغير عدد ساعات استخدام مواقع التواصل الاجتماعي في اليوم.

6.1 حدود الدراسة:

إنّ الدّراسة الحالية تحددت بمجموعة من الحدود، لعل من أهمها ما يلي:

الحدود الموضوعية: تقتصر الدّراسة في التعرف إلى علاقة مستوى الذكاء العاطفيّ بممارسة جرائم الابتزاز الإلكترونيّ لدى عيّنة من الضحايا في الضفة الغربيّة.

الحدود المكانية: تمّ تطبيق هذه الدّراسة في (وحدتي الجرائم الإلكترونيّة في الشرطة الفلسطينيّة والنيابة العامة، ووحدة حماية الأسرة في جهاز الشرطة الفلسطينيّة).

الحدود الزمانية: تمّ تطبيق هذه الدّراسة من العام الدراسي (2018/2017م) إلى العام الدراسي (2019/2018م).

الحدود البشرية: (208) ضحية لجرائم الابتزاز الإلكترونيّ في الضفة الغربية، حسب إحصائيات كلّ من (وحدتيّ الجرائم الإلكترونيّة، ووحدة حماية الأسرة، 2019).

الفصل الثاني

الإطار النظريّ

1.1 الذكاء العاطفيّ:

1.1.2 مقدمة:

في ظل التطور العلمي والتكنولوجي وسيطرة الماديّات على جميع مناحي الحياة وكافة الأصعدة الفرديّة، والأسريّة، والبيئية المحيطة والعلاقات المتبادلة فيما بينهم شاع في الآونة الأخيرة استخدام مفهوم "الذكاء العاطفيّ"، حيث يعتبر مصطلحا حديثا جاء نتيجة إدراك علماء النفس أهمية فهم الإنسان لذاته وللآخرين، وكيفية السيطرة على مشاعره وانفعالاته وكيفية توظيفها والتحكم فيها، حيث سعى العلماء إلى توظيف ما سبق في فهم شخصيّة الإنسان، وتنمية قدراته، ورفع مستوى عمله وإنتاجه، وإرساء قواعد تسهم في تكيف الإنسان داخل مجتمعه، ذلك الإنسان الذي لم يعد قادرا على تحمل ضغوط الحياة اليوميّة المتزايدة الناتجة عن التطور السريع والتحديث المستمر في كلّ مظاهر الحياة خاصة التكنولوجية والتقنية، حيث انتشر العنف وكثرت الجرائم والأمراض النفسيّة يوما بعد يوم بشكل أكبر، وبالتالي نتجت جرائم حديثة لم تكن موجودة سابقا مثل جرائم الابتزاز الإلكتروني (سلامي، 2016).

مما سبق نلاحظ أنّ الذكاء العاطفيّ يعطي توقعا لمدى نجاح الفرد بعدة أصعدة في حياته، لذا يجب تقديم الرعاية المتكاملة للفرد في جميع جوانب شخصيته من أجل صقلها ونموها نموا متكاملًا (جسميا، وعقليا، وعاطفيا، واجتماعيا)، وهذا ممّا لا شك فيه ينعكس على الفرد بنواحٍ إيجابية ويجعله قادرا على التفاعل السليم وتحقيق النجاح في أصعدة مختلفة سواءً أكانت أكاديمية أم مهنية، وأيضا تحقيق

التكيف النفسي والاجتماعي مما يجعله فردا يتمتع في مستوى ذكاء عاطفي عالٍ وسوي، وتتبع أهميته من إنَّ للطاقت البشرية دورا بالغ الأهمية في بناء الحضارة، من خلال الأشخاص القادرين على تحقيق النجاح والتقدم في حياتهم من ثم النهوض بمجتمعهم (الجعيد، 2011).

2.12 مفهوم الذكاء العاطفي:

تم التوضيح سابقا من خلال مقدمة الدراسة أنَّ لمصطلح الذكاء العاطفي عدة مفاهيم، ذلك بسبب اختلاف العلماء في ترجمة "Emotional intelligence"، لذا ظهر عدة مسميات منها: (الانفعالي، والوجداني، والمشاعر، والاجتماعي)، حيث يرى بعض العلماء أنَّ استخدام مصطلح الذكاء العاطفي يعتبر أكثر شمولية من الذكاء الوجداني والمشاعر نظرا لأنهم قد يمثلان المشاعر الإيجابية فقط، ممَّا سبق نلاحظ أنَّ مصطلح الذكاء العاطفي يعتبر أكثر شمولاً لكافة العواطف، وردود الأفعال، والانفعالات التي قد تكون سلبية وقد تكون إيجابية، وانطلاقاً من ذلك علينا إلقاء الضوء على مركبات مفهوم الذكاء العاطفي وتميزها، من ثم التعرف على مفهومه بالوجه الصحيح. (حسين ، وحسين ، 2006: 14)

الذكاء لغة: "الجذر الثلاثي "ذكا"، يشار له بأنه الذهن والحكمة" (خوالدة، 2004: 48).

وقد عُرف أيضاً بأنه "سرعة الفطنة والاستعداد التام لإدراك المعرفة والعلم" (عثمان، 2009: 59).

الذكاء اصطلاحاً: عرفه ديريون المُشار له في (ال عمران والعجمي، 2006: 239)، " بأنه القدرة على اكتساب الخبرات المختلفة والإفادة منها مع مراعاة الفروق الفردية بين الأفراد، باختلاف مستوى الذكاء (IQ) لديهم".

الذكاء إجرائياً: مجموعة من القدرات المتنوعة التي يستخدمها الفرد في حياته منها التحليل، التفسير، الإدراك، الانفعال، المشاعر، التكيف، حيث يتم استخدام هذه القدرات وفق ما يحتاجه الفرد لتفسير ما يحدث معه.

العاطفة لغة: "جاءت من الفعل الثلاثي عَطَفَ، حيث يقال فلان عطوف بمعنى أن يكون مرهف

الإحساس وغير عقلاني، ويقال رجل عطف أي حسن الخلق" (جروان، 2012:38).

العاطفة اصطلاحاً: "عبارة عن مجموعة من الانفعالات والميول التي تشكل نظاماً كاملاً متكاملًا، تساعد الفرد على التكيف لاتخاذ ردة فعل أو اتجاه معين، وقد تكون موجّهة نحو فرد أو جماعة أو فكرة" (المليجي، 1985: 154).

العاطفة إجرائياً: هي حالة من الشعور والانفعالات التي تحدث لدى الفرد، قد تكون إيجابية مثل: الحب والسرور، أو سلبية: مثل الكره والغضب، وفي كلتا الحالتين يتأثر الفرد فيهما ممّا يؤدي إلى قيامه برد فعل ما.

الذكاء العاطفي: تعددت وتنوعت المفاهيم الخاصة بمصطلح الذكاء العاطفي من قبل العلماء، ذلك لأنّ مدلوله ومضمونه واسعان، حيث يتضمن العديد من المهارات والمفاهيم والقدرات التي تميّز كلّ فرد عن الآخر، وله العديد من المؤشرات والمقاييس والجوانب (رشوان، 1990: 89).

وعرفه (ترمان، 1921) المُشار له في (رشوان، 1990: 54): " أنّه التفكير الذي يعتمد على التصورات والعمليات والرموز الذهنية، والقدرة على فهم معاني الأشياء لا الأشياء ذاتها، حيث يجتمع ما سبق ليكون القدرة على التفكير المجرد".

كما عرّفه (Bar-on, 2005: 41-62): "بأنّه مجموعة من المهارات الانفعاليّة الاجتماعيّة والشخصيّة التي تؤثر على قدرة الفرد على النجاح في مواجهة الضغوط المحيطة".

بينما عرّفه (عثمان، 2009، 162) " على أنّه قدرة الفرد على إدراك المشاعر وتوظيفها في اتخاذ القرارات الصحيحة في الحياة، وأيضاً القدرة على التعامل مع الضغوط والتحكم في الدوافع والانفعالات، بالإضافة إلى القدرة على التعاطف مع الآخرين ومعرفة ما يدور في داخلهم، وهو يمثل (المهارات الاجتماعيّة) التي تتمثل في التعامل مع الأفراد والتعامل مع مشاعرهم، ذلك من خلال بناء العلاقات الاجتماعيّة معهم والقدرة على قيادتهم وإقناعهم"

أمّا من وجهة نظر (ماير وسالوفي، 1990) المشار له في (الجعيد، 2011:7-8) يعرف الذكاء العاطفيّ بأنّه قدرة الفرد على مراقبة مشاعره وانفعالاته الذاتية وانفعالات ومشاعر الآخرين، والتمييز

بينهما وتوظيف المعرفة لتوجيه تفكيره وسلوكه بطرق صحيحة".

في حين عرّفه (جولمان، 2000: 11) " بأنه مجموع من المهارات الانفعالية والاجتماعية التي يتمتع بها الفرد والتي تؤدي إلى نجاحه في الحياة".

نلاحظ من التعريفات السابقة والمتنوعة للذكاء العاطفيّ أنّه مجموعة من القدرات والصفات الشخصية والاجتماعية، لذا يمكننا أن نستدل بأنهم يحملون في طياتهم عددا من السمات والصفات للأفراد ذوي الذكاء العاطفيّ المرتفع، لعل من أهمها التعبير عن المشاعر الإيجابية والسلبية والقدرة على تمييزها وتعريفها وإدارتها، وتحفيز الذات وإدارة الانفعالات وحل المشكلات، إضافة إلى التعاطف مع الآخرين وتفهم مشاعرهم وانفعالاتهم، إضافة إلى توظيف المشاعر والعواطف الذاتية من خلال تكوين علاقات اجتماعية وشخصية والموازنة بين مصالح الآخرين والمصالح الذاتية والموازنة بينهما.

3.1.2 التطور التاريخي لمفهوم الذكاء العاطفيّ ونشأته في علم النفس:

تعود الجذور التاريخية لمفهوم الذكاء العاطفيّ في مجال علم النفس إلى القرن الثامن عشر حسبما أشار إليه (ماير وسالوفي، 1997)، لكن بالإمكان اعتبار البداية الحقيقية كانت لجولمان، حيث قسم علماء النفس العقل إلى ثلاثة أقسام مختلفة، على النحو التالي:

- **القسم الأول: المعرفة:** تشمل على وظائف الذاكرة والعمليات المعرفية المتنوعة.
- **القسم الثاني: العواطف:** تشمل العواطف والمشاعر والانفعالات المتنوعة.
- **القسم الثالث: الدافعية:** تتضمن الدوافع البيولوجية أو المكتسبة.

بينما يرى العالمان ماير وسالوفي بأنّ ليس كلّ ما يربط المعرفة بالعاطفة هو ذكاء عاطفيّ، فالعاطفة هي " استجابة قد تكون إيجابية أو سلبية لحدث ما داخل الفرد أو أثناء تعامله مع الآخرين"، أمّا الذكاء، فقد عرفاه على " أنّه صفة تبين كيفية عمل المعرفة بحيث يستطيع الفرد التعلم والتفكير واتخاذ القرار والتكيف" (العلوان، 2011: 125).

وأشار (المللي، 2010) المشار له في (الجعيد، 2011: 6) إلى " أنّ الذكاء العاطفيّ له ثلاثة أقسام هي: المعرفة، الدافعية، الانفعال"، تتفاعل وترتبط مع بعضها البعض بالطرق السوية والسليمة فتؤدي إلى التفكير الإيجابي بالتالي الذكاء العاطفيّ.

مما سبق وبغض النظر عن المُسميات المختلفة التي تُطلق على "الذكاء العاطفي"، إلا أنّ نشأته مرتبطة بأسماء عدة علماء منهم (جولمان، 1990)، (بارون، 1997)، (ماير وسالوفي، 1997)، حيث مرّ مفهوم الذكاء العاطفيّ بعدة مراحل كانت أول مرحلة فيها تفصل بين التفكير والعاطفة فصلا تاما، ثم في الفترة الممتدة ما بين عام (1970-1990) بدا البحث عن العلاقة بين العاطفة والتفكير وتفسيرها، وفي عام (1994) ظهر مفهومه بشكل أوضح، فعلى الرغم من أنّ مفهوم الذكاء العاطفيّ يعتبر حديثا نسبيا إلا أنّ له تاريخا طويلا من الأبحاث في مجال علم النفس، والدليل على ذلك ما أكده العالم "ماير" كما أشرنا سابقا في أنّ أصل الذكاء العاطفيّ يعود إلى القرن الثامن عشر، حيث بات من المعروف لدى علماء النفس أن العقل الإنساني يتكون من ثلاثة أقسام: المعرفة، الوجدان، والدوافع كما تمّ التوضيح سابقا (Mayer, salovey, 2000:4-6).

ومن خلال القرن الماضي حاول بعض أنصار النظرية التقليدية للذكاء إدخال الانفعالات في مجال الذكاء منهم (ثورونديك، 1949) الذي قدّم نظرية عن الذكاء ميّز فيها بين ثلاثة أنواع من الذكاء، على النحو الآتي كما وضحتها (حسن، 2007: 18):

- 1- الذكاء المُجرد: يعني القدرة على التعامل مع الألفاظ والمفاهيم والرموز.
- 2- الذكاء الميكانيكي (العملي): يعني التعامل مع الأشياء.
- 3- الذكاء الاجتماعي: يعني مهارات التعامل مع الآخرين.

وفي سنة (1940) عزّف ويكسلر المشار له في (عبد الهادي، 2003: 49-59) الذكاء على أنّه "القدرة الشاملة والكاملة على التصرف والتفكير والتعامل مع البيئة المحيطة بفعاليّة وعقلانيّة.

وفي الفترة (1970-1989) تعرضت الانفعالات للبحث بشكل مكثف حيث انبثقت عن ذلك مجالات جديدة للبحث تناولت "المعرفة والوجدان"، ودراسة كيفية تفاعل الانفعالات مع الأفكار، الأمر الذي أسهم في ظهور العديد من الدراسات في الذكاء الصناعي (الرفاعي، 2012: 34).

وفي عام (1983) كما ورد في (الخوالدة، 2004: 29) بأنّ هوارد جاردينر أكّد في كتابه "أطر العقل"، الذي يرى فيه أنّ أحد أنواع الذكاء هو فهم الإنسان لنفسه وللآخرين وقدرته على استخدام وتوظيف هذا الفهم، حيث تحدث في كتابه عن نوعين متعلقين بالمظاهر اللامعرفيّة للذكاء وأعتبرهما مهمين أكثر

من الذكاء الذهنيّ وهما:

- **الذكاء الشخصي:** "يعني القدرة على معرفة الذات وضبطها، والقدرة على التصرف والوعي".
- **الذكاء البيئي:** "يعني القدرة على إدراك المشاعر ودوافع والحالات المزاجية للآخرين" (ابورياس واخرون، 2006: 228؛ جابر، 1993: 9)

أما في عام (1985) فتوصل عالم النفس " روبر ستيرنبرج" من خلال أبحاثه إلى نفس النتائج التي توصل إليها " ثورنديك"، والتي تفيد بأن الذكاء العاطفيّ يتميز عن القدرات العقلية والأكاديمية، إذ يجعلهم يتصرفون بحكمة اتجاه حياتهم (جولمان، 2000: 67).

وفي عام (1999) ظهر مصطلح الذكاء العاطفيّ لأول مرة على يد الأستاذين "سالوفي" من جامعة "ييل"، وماير من جامعة "همشابير"، حيث اعتبرا الذكاء العاطفيّ نوعا من أنواع الذكاء الاجتماعيّ، وعرفاه في تلك الحقبة على أنه " قدرة الفرد على تمييز مشاعره وانفعالاته وفهما ، ومن ثم استثمار هذه القدرة بالتفكير والسلوك بشكل صحيح" (Mayer, Salovey, 1990: 185-211).

وفي عام(1996) ظهر "جولمان " عالم النفس وأصدر كتابا بعنوان "الذكاء العاطفي"، قام فيه بجمع مجموعة من الأبحاث التي تناولت "تأثير مراكز المخ على انفعالات الفرد وعلاقاته مع الآخرين"، حيث كان له الفضل في انتشار مفهوم الذكاء العاطفيّ بشكل واسع بالتالي زيادة الأبحاث حوله (حسن، 2007: 22-23).

مما سبق من ذكر التطور لمفهوم الذكاء العاطفيّ ونشأته، قام العالم "ماير" بتلخيص تطور المفهوم في مراحل عدة بشكل مختصر، على النحو الآتي:

1. **المرحلة الأولى:** تميّزت باستخدام الدراسات النفسية للذكاء والانفعالات لمحاولة تعريف الذكاء العاطفيّ، امتدت هذه المرحلة ما بين (1900-1969).
2. **المرحلة الثانية:** ركز خلالها علماء النفس في دراساتهم على التأثير المتبادل بين الانفعالات والتفكير، امتدت هذه المرحلة ما بين (1970-1989).
3. **المرحلة الثالثة:** كانت أول ظهور حقيقي لمصطلح الذكاء العاطفيّ في العديد من المقالات

والدراسات، امتدت من عام (1990) إلى عام (1993).

4. **المرحلة الرابعة:** خلال هذه الفترة بدأ مفهوم الذكاء العاطفي بالانتشار بشكل واسع في عدة ميادين، وامتدت هذه المرحلة ما بين (1994-1997).

5. **المرحلة الخامسة:** امتدت هذه المرحلة من (1998) إلى يومنا هذا، إذ تمّ تعريف مفهوم الذكاء العاطفي بشكل أوضح مع زيادة الدراسات والكتابات حوله (Mayer, Salovey, 1990: 5-6).

4.1.2 أهمية الذكاء العاطفي في بعض مجالات العلوم العلمية:

لا تقتصر أهمية الذكاء العاطفي في مجال علم النفس، بل تتعدى أهميته إلى عدة مجالات علمية وحياتية مختلفة، منها في مجال الطب البشري حيث أثبتت بعض الدراسات أنّ قيام الفرد بالإفصاح عن الانفعالات والعواطف السلبية الضاغطة له يساعد على التقليل من حدة بعض الأمراض، منها الأورام السرطانية وأمراض القلب، إذ تبين أنّه يوجد صفة مشتركة لبعض مرضى السرطان والقلب، وهي تعمدهم لكبت عواطفهم وانفعالاتهم السلبية، وقد أظهرت الأبحاث أنّ الذكاء العاطفي يساعد في التخفيف من حدة كبت المشاعر والانفعالات السلبية، حيث يعمل على مساعدة الدماغ في التخلص من الشوائب السلبية التي تنتجها تلك العواطف (عدس وتوق، 2005: 40).

بينما في مجال التربية ساعدت الأبحاث التي تدرس الدماغ البشري في التوصل لنتائج مفادها أنّ الصحة العاطفية شيء أساسي وفعال للعملية التعليمية، حيث ذكر (جولمان، 2000: 56) عناصر العملية التعليمية الفعالة التي تسهم في الوصول للصحة العاطفية، لعل من أهمها يتمثل في الثقة وحب الاستطلاع، وضبط الذات، والانتماء، والقدرة على التواصل، والقدرة على التعاون، والقدرة على التكيف.

بينما في مجال الصحة النفسية توصلت الأبحاث والدراسات إلى نتائج مفادها أنّه عندما يصل الفرد إلى مرحلة الشعور بأنّه مستقل ولديه القدرة على التحكم في كلّ مواقف حياته بما فيها انفعالاته ومشاعره مع ذاته ومع الآخرين يكون بذلك قد حقّق التوازن الانفعالي ممّا يعطيه التوازن النفسي، لأنّ الحياة من دون العاطفة تصبح مملّة، لكن إذا كان الإنسان منجرا وراء انفعالاته ومشاعره دون التحكم الصحيح فيها، فقد تتحول إلى حالة مرضية كما في حالات القلق والاكتئاب والغضب (روبينس وسكوت، 2000: 134)، حيث تتضمن العاطفة العديد من المشاعر التي قد تكون إيجابية أو سلبية،

مثل (الحب الكراهية، السعادة، الخوف) (تشانج، 2002: 10).

بينما أشارت العديد من الدراسات إلى وجود علاقة بين الذكاء العاطفي والعديد من المتغيرات منها (قلة أمراض الاكتئاب، والإحباطات، وخفض السلوك العدواني، والأداء الدراسي) (محمود ومطر، 2002: 132).

5.1.2 مكونات الذكاء العاطفي:

يوجد العديد من الأبعاد والمكونات للذكاء العاطفي، حيث يعود هذا إلى تعدد وجهات نظر العلماء والباحثين كما ذكرنا سابقاً، مما نتج عنها العديد من النظريات والنماذج التي تفسره حسب وجهة نظر كلٍّ منهم وفهمهم لمفهوم ومكونات الذكاء العاطفي فمنهم من يرى أنه مجموعة من المهارات والقدرات التي يمتلكها الفرد، وآخرون يرون أنه الوعي والكفاية الشخصية، وهناك من يراها من وجهات نظر أخرى، فمكونات الذكاء العاطفي من وجهة نظر (سالوفي وماير، 1990) تتمثل في:

- **الوعي بالذات:** تعني وعي الفرد بمشاعره وانفعالاته وعواطفه وأفكاره المرتبطة بها وتعريفهم.
- **كبت الانفعالات:** تعني قدرة الفرد على التحكم في مشاعره وانفعالاته من ثم ضبطها وليس منعها بمعنى (تهديئة النفس).
- **الاستعداد الرئيسي:** تعني الطاقة الداخلية التي تؤثر بشدة في القدرات الإيجابية والسلبية وإعاقتها.
- **الفنون الاجتماعية:** أساس العلاقات مع الآخرين هو إدارة الانفعالات، حيث يتطلب التعامل مع مشاعر الآخرين ارتفاع مستوى مهارتين هما إدارة الذات والتعاطف مع الآخرين، إن القصور في إدارة الذات والتعاطف مع الآخرين يؤدي إلى تعرض الفرد إلى المشكلات المختلفة والمتنوعة.
- **التعاطف:** تعني القدرة على فهم وتفسير مشاعر الآخرين من خلال أصواتهم أو تعبيرات وجوههم، لتشمل الرسائل المباشرة وغير مباشرة التي يوجهها لغيرهم، فكلما كان الفرد على وعي بعواطفه وانفعالاته كان أكثر مهارة على قراءة مشاعر وانفعالات الآخرين، فالفشل في إدراك مشاعر الآخرين هو نقطة عجز أساسية في الذكاء العاطفي (محمد، 2009: 43-42).

في حين تتمثل مكونات الذكاء العاطفيّ وفق (جولمان، 2000) بالآتي:

- الوعي بالذات: تعني قدرة الفرد على فهم عواطفه وإدراكه مشاعره والقدرة على تمييزها.
- إدارة الانفعالات الذاتية: تعني قدرة الفرد التعامل مع المشاعر خاصة السلبية.
- الدافعية: تعني سعي الفرد نحو تحقيق "دوافعه" رغباته وأهدافه، يتم ذلك من خلال (الأمل، والمثابرة، والحماس، واستمرار السعي).
- معرفة عواطف الآخرين وفهما: تعني القدرة على قراءة رسائل الآخرين المباشرة وغير المباشرة المتمثلة في مشاعرهم، وانفعالاتهم، وصوتهم، وتعبيرات وجوههم، وحركة الجسد.
- إدارة الانفعالات: تعني القدرة على التفاعل مع الآخرين وفهم انفعالاتهم، وإدارتها من ثمّ حلّ المشكلات أي (المهارات الاجتماعية).

وأما مكونات الذكاء العاطفيّ من وجهة نظر (روبرت بار-اون، 1988) المشار لها في (أبو النصر، 2008: 110-111) تتمثل في:

- القدرة على معرفة المشاعر وتنظيمها وضبطها.
- القدرة على معرفة مشاعر الآخرين وفهم، والتأثر بها.
- الدافع الذاتي للعمل والإنجاز.
- القدرة على تكوين علاقات وثيقة وطويلة الأمد مع الآخرين.

6.1.2 سمات الأشخاص الأذكياء عاطفياً:

يوجد العديد من السمات التي يتصف بها الأفراد الأذكياء عاطفياً، لعل من أهمها حسب ما لخصها (محمد، 2009: 46-49) في أنه القدرة على إظهار مشاعره بوضوح وبشكل مباشر، ولا يخاف عندما يُعبر عن مشاعره، ولا تسيطر عليه العواطف السلبية مثل: الخوف، والقلق، والذنب، والخجل، والإحراج، وقادر على التعبير عن الانفعالات بدقة، وقادر على قراءة الاتصال غير اللفظي، ولا يخاف عند التعبير عن مشاعره وانفعالاته، ويترك مشاعره تقوده إلى الاختيارات الصحيحة التي تؤدي إلى سعادته، ومشاعره متوازنة مع الحق والمنطق والواقع، ويعمل وفقاً لرغبته وليس بسبب إحساسه بالواجب أو الذنب، وقادر على رفض أي خيار لا يناسبه، ومعتد على نفسه (مستقل)، ويحفظ جوهرياً ولا

يُحَفَّرُ بالقوة أو الثروة أو الشهرة، وقادر على أن يعرف المشاعر المتعددة، ويتكلم عن مشاعره بارتياح، ويهتم بمشاعر الآخرين، ويشعر بالتفاوت الواعي، ومتحدث مريح حول المشاعر، ويمتاز بالمرونة، ولا يتطبع بالفشل، وقادر على وضع الحدود بينه وبين الآخرين.

7.1.2 مقاييس الذكاء العاطفي:

يوجد العديد من المقاييس التي تهدف إلى قياس الذكاء العاطفي، نتيجة تنوع النماذج النظرية للذكاء العاطفي، حيث أشار كل من (أمرلينغ وجولمان، 2003) إلى أن هناك على الأقل ثلاثة مداخل مختلفة لقياس الذكاء العاطفي هي: مدخل القدرة، ومدخل السمات، ومدخل الكفاءة، وهذا ما يتفق مع تصنيف العالمين (ماير وسالوفي، 2000) لمقاييس الذكاء العاطفي حيث صنفت إلى ثلاثة أنواع هي:

أولاً: مقاييس القدرة: أوضح كل من "ماير وسالوفي" أن مقاييس القدرة تُعدّ مدخل لمعالجة المعلومات هذا في عام (2000)، حيث اهتمت هذه المقاييس بالقدرات المختلفة منها القدرة على التعبير، تهدف هذه المقياس إلى قياس قدرة الأفراد على حلّ مشاكلهم الانفعالية، ومن أهم تلك المقاييس حسب (حسن، 2007: 53-57) ما يلي:

أ. **مقياس الذكاء العاطفي متعدد العوامل:** أعداه "ماير وسالوفي" في عام (1998) حيث أوضح أن هناك علاقة وثيقة بين الذكاء العاطفي وقدرة الفرد على تجهيز المعلومات الوجدانية المرتبطة به، يعتبر أول مقياس لقياس الذكاء العاطفي، حيث اعتبر الذكاء العاطفي قدرة عقلية، إذ يتكون هذا المقياس من (12) مهمة، ويتضمن (114) مفردة تدرج تحت أربعة فروع للقدرات هي: الإدراك الانفعالي، والتسيير الانفعالي للتفكير، والفهم الانفعالي، وإدارة الانفعالات (موسى، 2012: 24).

ب. **اختبار (نموذج) الذكاء العاطفي:** قام كل من "ماير وسالوفي" بتحديث مقياس الذكاء العاطفي في عام (2000) متعدد العوامل الخاص بهما، حيث قاما بإدخال تحسينات على خصائص المقياس السيكومترية، يقيس هذا الاختبار قدرة الأفراد على إنجاز المهام وحلّ المشكلات الانفعالية كاعتراض على المقياس الذي يعتمد على تقييم الفرد الذاتي لمهاراته الانفعالية المدركة، تتمثل فروع اختبار (نموذج) الذكاء العاطفي كالاتي: الإدراك الانفعالي، والتسيير الانفعالي للتفكير، والفهم الانفعالي، وإدارة الانفعال (حسن، 2007: 56-57).

ثانياً: **مقاييس التقدير الذاتي:** أوضح" (بيتريدس وفورنهام، 2000)، أن مقاييس التقدير الذاتي قد تناولت الذكاء العاطفي كسمة، وفي هذا المقياس يُطلب من الفرد تحديد درجة انطباق مجموعة من التعبيرات الوصفية عليه، فإن كان مفهوم الفرد عن نفسه دقيقاً، فسيصبح تقديره لقدراته العاطفية الحقيقية دقيقاً والعكس، من أمثلة مقاييس التقدير الذاتي للذكاء العاطفي ما يلي:

أ. **قائمة نسبة الذكاء العاطفي بار- أون:** لقد أعدّ بار- أون عام (1991) قائمة لقياس الذكاء العاطفي أطلق عليها اسمه، واعتمدت على التقرير الذاتي للفرد، إذ تتضمن القائمة خمسة أبعاد رئيسية هي:

- **القدرات الشخصية، وتتضمن:** الوعي بالذات، والتوكيدية، واعتبار الذات، وتحقيق الذات، والاستقلالية.
- **القدرات الاجتماعية، وتتضمن:** المسؤولية الاجتماعية، والعلاقات الاجتماعية.
- **إدارة الضغوط، وتتضمن:** تحمل الضغوط، وضبط الاندفاع.
- **التكيفية، وتتضمن:** حلّ المشكلات، والمرونة، التكيف.
- **المزاج العام، ويتضمن:** التفاؤل، والحزن، والسعادة.

يتم تطبيق هذه القائمة على الأفراد من (16) عاماً أو أكثر، والهدف منها تقييم قدرة الفرد على النجاح في التعامل مع متطلبات وضغوط البيئة المحيطة والتكيف معها، و تتمّ الإجابة على الأسئلة أو المفردات من خلال مقياس متدرج من خمس نقاط تتراوح ما بين (نادراً جداً، ليس صحيحاً، صحيحاً غالباً، يحدث ذلك الأمر، أحياناً، مطلقاً) (Baron & Parker, 2000).

مما سبق نجد أنّ اختبار (نموذج) الذكاء العاطفي لماير وسالوفي يُعدّ الأنسب لقياس مستوى الذكاء العاطفي لدى الضحايا ذلك لأنها تتضمن العديد من الأبعاد والقدرات التي تسهم في أن يكون مفهوم الذكاء العاطفي واضحاً بشكل أكبر لدى الأفراد، حيث إنها لم يركز على جانب واحد من الأبعاد والقدرات والإمكانيات بل شمل جميع الجوانب لتتضمن القدرات الشخصية للفرد من وعي بذاته وتحقيقها واستقلاليته، القدرة على التعبير والانفعال وتوظيفها، وقدراته ومهاراته الاجتماعية وعلاقته بالآخرين، وقدرته على إدارة ضغوطه، حلّ مشكلاته، ليكون الأشمل والأنسب لهذه الدراسة لأنّ الفرد لا يكون بمعزل عن الآخرين في المجتمع ولا تخلو حياته من المشاكل وتغيرات المزاج العام له، لذا

هو بحاجة إلى ذكاء عاطفيّ ليكون قادر على التكيف مع كلّ التغيرات في حياته سواء على صعيده الشخصيّ أو على الصعيد التفاعليّ مع الآخرين.

ب. اختبار جولمان (1995): يتكون من عدة مواقف: (الوعي بالنفس، والتعرف على الشعور وقت حدوثه، والقدرة على تهدئة النفس،... إلخ) على الفرد أن يحدد استجابته في كلّ موقف من تلك المواقف، إذ تمثل استجابات الفرد على تلك المواقف تقريراً عن حاصل ذكائه العاطفيّ، حيث افترض "جولمان" أن هناك إجابة واحدة صحيحة على كلّ موقف من المواقف كلّما ازدادت الإجابات الصحيحة للفرد، ازدادت درجته في الذكاء العاطفيّ (السمادوني، 2007: 113)

ج. خريطة الحاصل الوجداني: أعدّ (Cooper, Sawaf, 1997) خريطة الحاصل الوجداني، قسماً فيها الذكاء العاطفيّ إلى خمسة مكونات هي:

- بيئة التعامل: تقيس قدرة الفرد على تحمل ضغوط الحياة ورضاه عنها.
- المعرفة الوجدانيّة: تقيس وعي الفرد بانفعالاته الذاتية وبنفعالات الآخرين، وقدرته على التعبير الانفعالي.
- الكفاءات المرتبطة بالحاصل الوجدانيّ: يقيس المرونة والإبداع والقدرة على بناء العلاقات مع الآخرين.
- الاتجاهات والقيم المتعلقة بالجوانب الوجدانيّة: يشمل بعد الأفق، و الشفقة، و الحدس، والنقّة، وقوة الشخصية، والذات المتكاملة.
- مخرجات مجال خريطة الحاصل الوجدانيّ: تقيس نتائج محددة للذكاء العاطفيّ مثل: الصحة العامة، والمكانة الاجتماعيّة في الحياة، ومحصلة العلاقات.
- د. قائمة شوت وآخرون (1998): صمّمها كلّ من (شوت، مالوف، هل، هق رتي، جوبر، جولدن ودورنهييم)، قائمة لقياس الذكاء العاطفيّ بأسلوب التقرير الذاتي معتمدين على مقياس "ماير وسالوفي"، تقيس أربعة أبعاد هي: التقويم والتعبير عن الانفعالات، وتنظيم الانفعالات، واستخدام الانفعالات في حلّ المشكلات، وفعاليات معرفيّة أخرى (الوشلي، 2003: 89).

ثالثاً: **مقاييس التقدير الملاحظ للذكاء العاطفي**: يعدّ مدخل التقدير الملاحظ من المداخل التي تتأثر بالعديد من الأشياء والتعبيرات الشخصية والمعتقدات المتعلقة بكيفية إدراك الفرد لشخصيته ومدى قدرتهم على تنظيم المعلومات، حيث يعتبر هذا المدخل مناسباً لقياس رؤية الملاحظين وليس لقياس القدرة العقلية للفرد لأنه لا توجد نتائج سلوكية ثابتة تدعم هذا التوجه، من أمثلة مقاييس تقدير الملاحظ أو المقاييس المتعددة على مدخل المعلومات هي:

أ- **قائمة الكفاءات الوجدانية**: الكفاءة الوجدانية هي عبارة عن "القدرة القائمة على الذكاء العاطفي التي تظهر في الأداء البارز في العمل، صمم كلّ من (بويتزس وجولمان وريه، 1999) "قائمة الكفاءة الوجدانية لقياس (20) كفاءة تندرج تحت أربعة جوانب للذكاء العاطفي هي:

- **الوعي بالذات**: يتضمن مقياس الوعي الانفعالي للذات، والتقييم الدقيق للذات، والثقة في الذات.
- **إدارة الذات**: يتضمن مقياس التحكم في الذات، الموثوقية، وبقظة الضمير، والتكيفية، ودافعية الإنجاز.
- **الوعي الاجتماعي**: يتضمن مقياس تعاطف الوعي التنظيمي، توجيه الخدمة.
- **إدارة العلاقات الاجتماعية**: يتضمن مقاييس تطوير الآخرين، والقيادية، والتأثير، والتواصل، وإدارة الصراع، وبناء العلاقات، وفريق العمل، والتعاون.

ب- **استبيان تقدير الذكاء العاطفي**: صمم كلّ من "برادبييري وقريفز وايمرلنغ" استبانة لتقدير الذكاء العاطفي بناء على نموذج "جولمان" الذي يتضمن الوعي بالذات، وإدارة الذات، والوعي الاجتماعي، وإدارة العلاقات الاجتماعية، وتم بناء أسئلة الاستبانة باستخدام مقياس متدرج سداسي (أبداً، نادراً، أحياناً، عادة، غالباً، دائماً)، ولهذا الاستبانة ثلاث نسخ هي حسب (حسن، 2007 : 61-63):

- 1) نسخة التقييم الذاتي.
- 2) نسخة التقييم المتعدد.
- 3) نسخة تقييم الذكاء العاطفي للفريق.

8.1.2 النظريات المفسرة للذكاء العاطفي:

هناك العديد من النظريات والنماذج العلمية المفسرة للذكاء العاطفي والموضحة للمهارات والسمات والقدرات المرتبطة به، حيث قدم العلماء العديد من المقاييس والنماذج حسب أبعاد كلّ نظرية، إذا يعتبر هذا التعدد في وجهات النظر دليل على الأهمية البالغة له، بالإضافة إلى ذلك نلاحظ أنّه تمّ استخدامه في العديد من المجالات العلمية كالمجالات: (النفسيّة، والتعليميّة، والتربويّة، والطبيّة)، ولعل من أهم تلك النظريات ما يلي:

1) نظرية بار-أون: تُعدّ نظريته أولى النظريات التي فسرت الذكاء العاطفيّ عند ظهورها عام (1988)، حيث توضح هذه النظرية أنّ الفرد الذي يتمتع بالذكاء العاطفيّ ومكوناته التي تتمثل في (الاستقلالية، وإدراك الواقع الذي يعيشه، وتحمل الضغوط، والقدرة على حلّ المشكلات، وضبط الاندفاع، والتحكم في الذات)، يكون لديه المقدرة على تحقيق ذاته وتقديرها ويتمتع بمستوى ذكاء عاطفيّ وسويّ، ومن لا يتمتع بها يكون لديه تدني ذات منخفض، الأمر الذي يجعله يتصف بأنّه انكالي لا يتحمل الضغوط، ولا يستطيع حلّ مشكلاته، إضافة إلى أنّه يتبع أساليب غير مشروعة للهروب من الواقع الذي يعيش فيه. ولعل أهم تلك الأساليب استخدام الشبكة العنكبوتية لتكوين شخصية وهمية يطمح إليها بالواقع، لكنّ ذلك قد يوقعه يوما ما ضحية لجرائم الابتزاز الإلكترونيّ، فينتج عن ذلك عدم القدرة على إدراك الواقع ومواجهة جرائم الابتزاز الإلكترونيّ ليكون أحد أطرافها، بسبب شخصيته في الواقع وشخصيته في الشبكة العنكبوتية والازدواجية التي يعيشها، هذا ما أشارت إليه هذه النظرية بتداخل الذكاء العاطفيّ مع سمات الشخصية، حيث أوضح بار-أون في نظريته أنّ الذكاء العاطفيّ يتكون من خمس كفاءات (قدرات) لا معرفيّة مقسمة إلى (شخصية، وكفاءات ضرورية للعلاقة بين الأشخاص، وكفاءات ضرورية لقابلية التكيف، وكفاءات ضرورية للقدرة على إدارة الضغوط، والتحكم فيها وإيجاد حلول) (السمادوني، 2007: 103-105).

• **نظرية ماير وسالوفي:** بدأ اهتمام الباحثين بهذا الموضوع منذ عام (1990) وتمّ إعداد أداة تجريبية لقياس الذكاء العاطفيّ، لكن عام (1997) يعتبر البداية الحقيقية لظهور وتطور هذه النظرية وأداة قياسها، حيث كان الهدف تطوير النظرة للذكاء العاطفيّ وتحليل مكوناته وإعداد أدوات قياس تقيسه كقدرة عقلية وليس كسمة شخصية، إذ أتت هذه النظرية لقياس الفروق الفردية حيث يرى العالم أن

المقاييس التقليدية للذكاء فشلت في دراسة الفروق من حيث (الوعي الذاتي، والإدارة الفعالة للعواطف، والمعلومات العاطفية الذاتية أي الاستجابات، وفهم ردود الأفعال)، من هنا يُعتبر هذا النموذج نموذجاً لتحليل الذكاء العاطفيّ لأنه اتخذ "منحنى القدرة"، وأجريت عليه بحوث من قبل الباحثين أو بالاشتراك مع آخرين مثل جارسو، فالذكاء العاطفيّ لديهما يعني "القدرة على إدراك وفهم المشاعر والانفعالات والتعبير عنها وتفسيرها في الذات والآخرين"، قسمت هذه النظرية الذكاء العاطفيّ إلى (إدراك العواطف، واستثمار العواطف، وفهم العواطف، وإدارة العواطف) (Mayer, Salovey, 1997).

3-34:

مما سبق نلاحظ أنّه عند قيام الفرد بالموازنة بين عواطفه وردود أفعاله، وبين الاستجابة وفهم الآخرين الذين يتعامل معهم لا ينجّر وراء عواطفه ويكون لديه القدرة على فهم العواطف، وإدراكها، واستثمارها للقيام بأنشطة إدراكية مثل حلّ مشكلاته، وبالتالي إدارة العواطف، ممّا يقيه من الوقوع في فخ جرائم الابتزاز الإلكترونيّ التي تلعب على وتر العاطفة لدى الضحية الذي يفتقر للذكاء العاطفيّ، فالشخص الذكي عاطفياً حسب "ماير وسالوفي" أفضل من غيره في التعرف على الانفعالات سواء كانت انفعالات الشخص ذاته أم انفعالات الآخرين، ولديه القدرة على التعبير العاطفيّ بصورة واضحة ودقيقة.

• **نظرية جولمان:** قدم نموذجه من خلال كتابه الذي نشره بعنوان "الذكاء العاطفي" عام (1995)، حيث حدد العديد من المهارات الانفعالية والاجتماعية التي يتمتع بها الفرد والتي تساهم في نجاحه في حياته والابتعاد عن المشاكل أو سوء الفهم الذي قد يوقعه ضحية للمبتزين الذي قد يستغلون عدم قدرته على إدارة عواطفه أي عدم تمتعه بالمعرفة الكافية في التعامل مع المشاعر التي تؤذيه، أو عدم وعيه الانفعالي بعواطفه ومشاعره الذاتية التي قد تضره وتؤثر على ردود أفعاله (حسين وحسين، 2006: 60).

مما سبق يتضح أنّ جولمان قام بتقسيم الذكاء العاطفيّ إلى خمسة أبعاد تحمل شقين: الشق الأول هو: الفرد، والشق الثاني هم: الآخرون، فمنّ يكن لديه وعي (بعواطفه الذاتية، وإدارتها، والدافعية، والتعاطف، والمهارات الاجتماعية)، يكن لديه القدرة على الموازنة في تحقيق ما سبق مع ذاته ومع الآخرين، ويتمتع بارتفاع مستوى الذكاء العاطفيّ لديه، وبالتالي يكون مدركاً وقادراً على التعامل مع

ذاته ومع الآخرين، بسبب قدرته على (معرفة المشاعر، وتحمل الضغوط، وقراءة عواطف الآخرين، والوعي بالقوانين المنظمة في المجتمع أي العادات والتقاليد)، وبالتالي لا يكون فريسة سهلة لأي كان سواء في التعامل بالحياة الواقعية أو بالواقع الإلكتروني الذي صممه لذاته (جولمان، 2000: 130-185).

• **نظرية ديسك:** جاءت هذه النظرية من الدكتور ويليام مارستون في كتابه (انفعالات الأشخاص العاديين) عام (1928)، وضح فيه عن كيفية التعرف على الأشخاص من خلال تحديدهم إلى أربع فئات، حيث ركز مارستون على الظواهر النفسية القابلة للملاحظة والقياس بصفة مباشرة، ورمز لهذه الفئات الأربعة بـ: السيطرة (D)، والدافع (I)، والخضوع (S)، والالتزام (C)، وسميت هذه النظرية ديسك (DISC) اختصاراً للكلمات الأربع (باوزير، 2016).

مما سبق نلاحظ بان الدكتور ويليام مارستون قد قسم الأفراد وفقاً لسلوكياتهم وطباعهم إلى أربع فئات منها: (المسيطر): وتعني بأنه شخص حازم وعملي ويحاول جاهداً بأن يكون مسيطراً على مجرى أمور حياته وحياة الآخرين، (الدافع) الشخص الذي يمتاز بأنه عفوي ومدفع في أسلوب حياته، و(الخاضع): وتعني بأنه شخص مخلص في أمور حياته لكن قد يوصله ذلك إلى الخضوع في بعض الأحيان، وأخيراً (الملتزم): وتعني بأنه شخص قادر على تحليل المواقف بدقة، وحذر في التعاملات المختلفة، ومن خلال هذه الأنماط بالإمكان أن يتضح لنا أي الأنماط قد تتفق مع شخصية الضحية ومدى قدرتها في التعامل مع ذاتها والآخرين، إذ من الممكن أن تتمتع الضحية بنمط شخصية متساهلة وعفوية ومدفوعة في تعاملها مع الآخرين مما يشكل عليها خطر الوقوع كضحية لجرائم الابتزاز الإلكتروني، في المقابل قد تتمتع الضحية بنمط شخصية الخاضع التي تكون متساهلة في قراراتها وتعاملاتها مع نفسها من جهة ومع الآخرين من جهة أخرى، ليقوم الجاني الذي قد يتمتع بنمط شخصية المسيطر باستغلال الاندفاع وعدم الحذر في التصرفات لإخضاع الضحية لطلباته المتكررة والمستمرة.

2.2 جرائم الابتزاز الإلكتروني:

1.2.2 مقدمة:

يعيش العالم المعاصر ثورة معرفية وتكنولوجية هائلة، هذه الثورة صاحبها انتشار العديد من التقنيات الحديثة منها الحاسب الآلي، والشبكة العنكبوتية (الإنترنت)، والأجهزة الذكية، التي أصبح استخدامها أمراً ضرورياً وملحاً لا غنى عنه في أداء الكثير من الوظائف والمهام، سواء على مستوى الفرد أو المؤسسة أو المجتمع، مما أدى إلى زيادة عدد مستخدمي هذه التقنيات بشكل كبير.

ولكن على الرغم مما تحمله هذه التقنيات التكنولوجية الحديثة من تسهيلات وإمكانيات هائلة سهلت على الإنسان الوقت والجهد والمال، فإن البعض قد أساء استخدامها، وهو ما أدى إلى إشاعة نمط جديد من الجرائم، وهو ما سمي بالجرائم الإلكترونية، التي تختلف في شكلها ومضمونها ووسائلها عن الجرائم التقليدية حيث تُعدّ جرائم ناعمة، لعدم وجود أسلحة أثناء تنفيذها، ولا يتم استخدام القوى البدنية لتنفيذها، هذا النوع من الجرائم عادة ما ينتشر بين فئة الشباب، بل وامتد إلى طلاب المدارس الأصغر سناً، لكنها في ذات الوقت تتمتع بذات أركان الجرائم التقليدية.

حيث يتضح لنا من خلال الإحصائيات العديدة المنتشرة أن هناك (978) مليون ضحية للجرائم الإلكترونية في (20) دولة حول العالم حتى عام (2017) منهم (353) مليوناً في دولة الصين، حيث تأثر ما يقارب (44%) من مستخدمي الإنترنت من هذه الجرائم خلال العام (2016) في العالم، وتتنوع هذه الجرائم ما بين سرقة الهوية الإلكترونية (الشخصية) أي الحصول على معلومات شخصية حول مستخدمي الإنترنت ومواقع التواصل الاجتماعي، واختراق الحاسب الآلي بهدف سرقة المعلومات أو التخريب، أو الحصول على الأموال من خلال الاحتيال والسطو على أرقام البطاقات الائتمانية (يماني، 2017).

بعد الانتشار الواسع لاستخدام التقنيات الحديثة من أجهزة ذكية ومواقع التواصل الاجتماعي انتقل العديد من الأفراد بتواصلهم وتفاعلهم من العالم الواقعي إلى العالم الافتراضي الإلكتروني، بالتالي انتقلت الجرائم لهذا العالم نتيجة الاستخدام الخاطئ، ولنا أن نتصور حجم التفاعلات التي تتم في الواقع الافتراضي سواء كانت شخصية أم مؤسسية أم خدماتية أم ثقافية، مما خلق فرصاً جديدة وسهلة للجناة في العالم الافتراضي الإلكتروني مما نتج عن ذلك نوعاً جديداً من الجرائم تسمى الجرائم

الإلكترونيّة، لا تقتصر على نوع واحد من الجرائم بل تتنوع وتتعدد أشكالها، فمن ضمن تلك الجرائم جريمة الابتزاز الإلكترونيّ (Wall,2007:15).

مما سبق نلاحظ أن جريمة الابتزاز الإلكترونيّ تُعدّ سلوكاً إجرامياً يتبعه الجاني لارتكاب جريمته، حيث يتمتع الجاني بالذكاء العالي عند اختياره للضحية، فيقوم بتتبعها ومراقبتها على مواقع التواصل الاجتماعيّ، من ثم القيام بالتواصل مع الضحية لمحاولة إيقاعها في فخه سواء من خلال علاقة عاطفيّة، أو علاقة صداقة، أو التحايل، أو اختراق الحساب وجهاز الضحية مباشرة خاصة للأفراد ذوي الياقات البيضاء في المجتمع، حيث تنوعت الأساليب المتبعة في جرائم الابتزاز الإلكترونيّ لديهم.

لذا عند تعريفنا للجرائم الإلكترونيّة في الغالب نعتد على الغرض من استخدام هذا المصطلح، إذ يشمل عدداً محدداً من الأعمال الإجراميّة ضدّ السرية والنزاهة وتوافر بيانات الكمبيوتر أو الأنظمة، ويمثّل جوهر الجرائم الإلكترونيّة أبعد من هذا الوصف، ومع ذلك فهي تشمل الأعمال الإجراميّة ذات الصلة بالحاسب الآلي والأجهزة الذكيّة لتحقيق أغراض شخصيّة أو تحقيق مكاسب ماليّة أو ضرر للغير، بما في ذلك أشكال الجرائم المتصلة بالهويّة الإلكترونيّة (الشخصية)، والأفعال المتعلقة بالعبث بمحتويات الحاسب الآلي (UNODC, 2013).

2.2.2 مفهوم جرائم الابتزاز الإلكترونيّ:

تعتبر جرائم الابتزاز الإلكترونيّ نوعاً من أنواع الجرائم الإلكترونيّة، لذا علينا أن نلقي الضوء على مكونات مفهوم جرائم الابتزاز الإلكترونيّ من خلال تفكيكها وتوضيح كلّ مفهوم منها على النحو الآتي:

الجريمة من وجهة النظر الدينية "خطيئة"، أي الخروج عن النظام الذي يعتقد أنّه من وضع الله أي "الدين". ومن وجهة نظر علم النفس: "هي إشباع الفرد غرائزه الإنسانيّة بطرق شاذة وغير سوّيّة، وحين يقوم بتلك الأفعال تشبع الغريزة نفسها، ذلك لأحوال نفسية شاذة انتابت مرتكب الجريمة في لحظة ارتكابها بالذات" (عوض، 2004: 5).

في حين أنّ علم الاجتماع يُعرفها على أنّها: "نوع من أنواع الخروج عن قواعد السلوك التي حدّدها المجتمع لأعضائه، حيث يجرّم أنواع السلوك التي فيها خروج وانحراف عن النظم التي وضعها المجتمع والسلطة العليا، إذ تُعدّ تهديداً لكيان المجتمع" (عوض، 2004: 18-25).

بينما تعرف من وجهة نظر القانون: "كلّ فعل يعود بالضرر، أو التهديد، أو الخطر على المجتمع ويقر له القانون عقوبة جنائية أو جزائية" (عوض، 2004: 6).

في حين عرفها (العباينة، 2010: 18) بأنّها "كلّ فعل عمديّ ينشأ عن الاستخدام غير المشروع للتقنيّة المعلوماتيّة، ويهدف إلى الاعتداء على الحقوق الماديّة والمعنويّة للطرف الآخر سواء أكان فرداً أم مؤسسة أم مجتمعا".

الإبتزاز لغةً : "جاء البزّ بمعنى السلب، وعند القول ابتزرت الشيء أي استلبته، الجذر الثلاثي بزّ" (مسعود، 1992: 171).

الإبتزاز اصطلاحاً: "تهديد شخص وإجباره بالإكراه على فعل ما للحصول على ماله، أو منفعة معينة" (بن شلهوب، 2011: 9).

كما يمكن تعريفه بأنّه: "جريمة يقوم بها الجاني بتهديد الضحيّة بشكل دائم ومستمر، عن طريق سلب إرادته والتحكّم فيه لتنفيذ مطالبه ورغباته، لذلك تُعدّ جريمة غير شرعية وسلوكاً غير سويّ ولا أخلاقي" (العنزي، 2010: 70).

كما عرفها (المطيري، 2015: 13): "هو الوصول إلى معلومات سرّيّة خاصة، والتهديد بإفشاء هذا السرّ الذي قد يلحق الضرر به بقصد الحصول على مكاسب ماديّة أو معنويّة من شخص معين بالإكراه والإجبار".

الإبتزاز إجرائياً: حصول الجاني على صور، أو فيديو، أو معلومات تخصّ الضحيّة واستغلالها من خلال تهديد الضحيّة بالفضيحة والإشهار، ذلك لإرغامها على تنفيذ طلبات الجاني التي قد تكون ماديّة أو أعمال غير مشروعة.

الجرائم الإلكترونية: أشار إليها (السراني، 2009: 26) بأنها "استخدام الحاسوب وتقنياته في عملية الاختراق والتعدي على البيانات والملفات والمعلومات بسرقتها أو العبث بمحتواها وتزويرها بطرق غير مشروعة".

الشبكة العنكبوتية (الإنترنت): "هي عبارة عن شبكة تميّزت بكونها وسيطا للاتصال يتميز بالتفاعلية، بحيث إنها تقوم بتحقيق التزامن وتغذية راجعة من خلال بعض أدواتها الاتصالية كالدرشة، أو من خلال المحادثات الجماعية، ويطلق على هذا النوع من الاتصال المتزامن" (Flew, 2003: 21).

وقد عرّفها (نصر، 2015: 4) بأنها "شبكة حواسيب عالمية ترتبط مع آلاف الشبكات وملايين أجهزة الحاسب الآلي في نظام يتألف من مزودات للخدمة تدعم مستندات ذات تنسيق خاص".

الابتزاز الإلكتروني اصطلاحاً: "استخدام التهديد لإرغام شخص على التوقف عن عمل مسموح به عادة أو إرغامه على فعل ما لا يريد، ويرتكز أسلوب الابتزاز على عنصر الإكراه والتهديد" (السعدون، 2008: 64).

الابتزاز الإلكتروني إجرائياً: هي جرائم يمارسها الفرد من خلال أجهزة الكمبيوتر والهواتف الذكية، لسرقة معلومات خاصة بالضحية، والإيقاع بها من خلال الشبكة العنكبوتية (الإنترنت)، من ثم تهديدها وابتزازها بالمعلومات التي تمّت سرقتها مقابل عدم الفضيحة للوصول إلى أهدافه التي خطط لها.

بناء على ما سبق يمكن القول: إنّ الجرائم الإلكترونية هي كلّ فعل يتمّ به استخدام نوع من أنواع الحاسب الآلي أو الهاتف المحمول الذكيّ أو الشبكة العنكبوتية (الإنترنت) أو مواقع التواصل الاجتماعيّ لتسهيل ارتكاب جريمة أو عمل مخالف للقانون، إذ يعدّ الابتزاز الإلكترونيّ أحد أنواع الجرائم الإلكترونية.

3.2.2 التطور التاريخي لجرائم الابتزاز الإلكتروني:

نشأت جرائم الابتزاز الإلكترونيّ نتيجة التطورات والتغيرات السريعة والمستمرة في التقنيات التكنولوجية، لذا يوجد صعوبة في تحديد بداية معينة لبدائها، إلا أنّ البعض يرجح حدوث أول جريمة متصلة بالحاسب الآلي إلى عام (1801) عندما قام صاحب مصنع للنسيج في فرنسا بتصميم لوحة إلكترونية

تقوم هذه اللوحة بتكرار مجموعة من الخطوات المستخدمة لحياكة أنواع من المنسوجات، الأمر الذي جعل بعض العاملين في المصنع خائفين من تأثيرها على عملهم مما دفعهم إلى تخريبها، بينما يرجع البعض الآخر البداية الحقيقية لظاهرة الجرائم الإلكترونية إلى عام (1985) حينما بدأ رصد بعض الحالات التي أطلق عليها "إساءة استخدام الحاسب الآلي" ذلك من خلال معهد ستانفورد الدولي للأبحاث في الولايات المتحدة الأمريكية (السرحاني، 2014: 12).

تطورت الجرائم الإلكترونية عبر التاريخ بعدة مراحل منذ بداية رصدها في الإحصائيات لأول مرة في الفترة من عام (1971) إلى (1990)، حيث تراوح عددها بين جريمة واحدة إلى ثلاث جرائم خلال العام، أشهرها كان في عام (1988) عندما تم استخدام الحاسب الآلي لسرقة (70) مليون دولار من بنك شيكاغو الوطني، وفي ذات العام تم تكوين فريق طوارئ الحاسب الآلي في معهد هندسة البرمجيات بجامعة كارنيجي ميلون الأمريكية لمواجهة الجرائم الإلكترونية بأنواعها وأشكالها المتعددة والمتنوعة (Council of Europe, 1989).

وفي التسعينيات أصدرت عددا من الحكومات تشريعات لمحاولة التصدي للجرائم الإلكترونية، تحديدا في ظل الإحصائيات المتوفرة عن استخدام الإنترنت في تلك الفترة، حيث شهد العام (1993) (14,161,570) مستخدما علما أن عدد سكان العالم في العام نفس كان (5,578,865,11) مليارا، ليتضاعف عدد المستخدمين ليصل في عام (1999) إلى (280,866,670) مليون مستخدم بعد أن وصل عدد سكان العالم إلى (6,05,478,010) مليار نسمة في ذلك العام (القحطاني، 2014: 30-31).

وحدثت تطورات كثيرة ومتسارعة في الفترة الواقعة ما بين عام (2000) وعام (2014)، حيث ارتفع أعداد مستخدمي الإنترنت وبالتالي ارتفعت معه معدلات الجرائم الإلكترونية، لينتج عنها خسائر مالية ضخمة على عدة أصعدة، فأصدر مجلس أوروبا عام (2001) اتفاقية مجلس أوروبا للجريمة الإلكترونية، لكن تم التأخير في تصديق هذه الاتفاقية وتنفيذها مما نتج عن هذا التأخير آثار سلبية بالغة أهمها زيادة نسبة الجرائم الإلكترونية بشكل كبير وضخامة الخسائر المادية وتعقيد طرق مواجهتها (Number Internet Users, 2014).

وفي عام (2002) وصل عدد مستخدمي الإنترنت (662,663,600) في حين بلغ عدد سكان العالم (6,280,853,820) لتعادل زيادة استخدام الإنترنت (32%) عن العام (2001)، حيث تم إصدار مرشد من خلال منظمة التعاون الاقتصادي والتنمية لأمن نظم المعلومات والشبكات، بينما في العام (2019) وصل عدد مستخدمي الإنترنت حول العالم إلى (4,100,667,287) مستخدم (ليدك، 2019).

وبمرور الزمن وتطور التقنيات والتكنولوجيا نتج أنواع جديدة من أنواع الجرائم الإلكترونية من ضمنها جرائم الابتزاز الإلكتروني، لكن في البداية علينا تتبع تاريخ الابتزاز، إذ يوجد العديد من جرائم الابتزاز التي حصلت عبر التاريخ، حيث كانت عبارة عن جرائم ابتزاز مجردة تقوم على الإكراه والتهديد للضحية وإرغامه على تلبية وإشباع رغبات الجاني، قد يحمل الإكراه شقين: نفسي وجسدي، فالنفسى يكون من خلال الضغط والترهيب النفسى للضحية، أمّا الجسديّ، فيتمثل في التهديد بالضرب والسجن والقتل (الحري، 2011 : 76).

ويمكن القول: إن فكرة الابتزاز قديمة بقدم التاريخ، الدليل على ذلك قصة سيدنا يوسف عليه السلام وامرأة العزيز، حيث راودته عن نفسها ورفضها خوفاً من الله، فهددته بالسجن إن لم يخضع لطلبها، وكانت النتيجة اختياره السجن على معصية الله معها (ابن منظور، 1990: 386)، "وقصة ذي الكفل من بني إسرائيل حينما أراد أن يعاشر امرأة فأعطاها ستين ديناراً، فلما همّ إلى ذلك بدأت في البكاء، فسألها ما بك؟ فقالت: لم أقم بهذا في حياتي، فسألها: لماذا؟ فقالت: دفعتني الحاجة، فتركها وأعطاها الدنانير دون مقابل" (الجوزية، 2001: 265).

نلاحظ ممّا سبق أنّ ظاهرة الابتزاز منتشرة منذ الأزل، خاصة الابتزاز الجنسيّ والنفسى المبنين على الإكراه والإرهاب بشكل كبير للضحية لإرغامها على الخضوع، حيث يوجد العديد من القصص التي توضح ذلك على مرّ التاريخ، في مرحلة لاحقة تحديداً في عام (1932) حدثت واقعة ابتزاز مالي مشهورة للأمريكي "شارلز لندبرغ" إذ كان معروفاً بأنه مخترع ومكتشف وطيار، حيث قام أفراد معينين بخطف ابنه من المنزل أثناء تواجده مع حاضنته، من ثم طلبوا المال مقابل الإفراج عنه لكن بسبب المروغات التي حدثت قاموا بقتله (العيسى، 2011: 265).

أما فيما يتعلق بالابتزاز الجنسي الذي كان منتشرا في المكاتب، فظهر كتاب الابتزاز الجنسي ليعالج هذه القضية ويوضحها، حيث نشرته لين فارليي عام(1978)، في بعض الحالات حين تعمل المرأة تحت إدارة رجل، أو مع رجال في المكان نفس ، قد تتعرض لابتزاز جنسي، على أثر ذلك نشر تحقيق صحفي عام(1980) في مجلة لنيوزويك بعنوان "سوء استخدام الجنس في المكاتب"، حيث ذكر العديد من القصص لاستغلال المدراء لموظفاتهن النساء مما قد يصل إلى الابتزاز الجنسي، ذلك حتى تبقى في وظيفتها أو تترقى أو تحصل على زيادة مالية، لذا لا يقمن بالتبليغ عن المبتز خوفا من خسارة عملهن(البار، 1987: 12-15)، وبتطور مفهوم جرائم الابتزاز نتج نوع آخر من الابتزاز إلا وهو الابتزاز الإلكتروني الذي يتميز في التهديد بالإشهار والفضائح للضحية(الحري، 2011: 77).

إنّ ما سبق يوضح لنا مفهوم الابتزاز بأنواعه وأشكاله المختلفة بشكل عام، لكن عند التطرق إلى الابتزاز الإلكتروني نجده مرتبطا ارتباطا وثيقا بالتطور التكنولوجي والتقني المستمر خلال القرنين: العشرين، والواحد وعشرين، الذي نتج عنه الشبكة العنكبوتية (الإنترنت) أساس استخدام مواقع التواصل الاجتماعي المنتشرة بشكل كبير لدى الأفراد في العالم، فمن خلالها يتم الاتصال والتواصل بين الأفراد المتواجدين على الشبكة الإنترنت سواء بالصوت والصورة، أو الفيديو، مما سبق نتوصل لنتيجة مفادها إذ تمّ استخدام الشبكة العنكبوتية ومواقع التواصل الاجتماعي بشكل صحيح هذا يعني حماية الأفراد والمجتمع من سلوكيات وممارسات تهدد أمنهم واستقرارهم، وإن تمّ استخدامها بشكل غير واعٍ وغير صحيح يُسهل ذلك وقوع الأفراد ضحايا لجرائم الابتزاز الإلكتروني المتنوعة من قبل بعض الأفراد ضعاف النفوس القادرين على استغلال غيرهم عاطفيا ومالياً.

4.2.2 أنواع جرائم الابتزاز الإلكتروني:

تعدّ جرائم الابتزاز الإلكتروني من السلوكيات السلبية والإجرامية التي تعتمد على عنصر الإكراه والإجبار لتنفيذ طلبات المبتز، حيث لا يشترط ممارسته ضدّ الرجال أو النساء بل يشمل الجنسين وشرائح عمرية مختلفة خلال فترات زمنية متعددة مختلفة، بأساليب وأنواع متجددة لعل من أهم تلك الأنواع ما يلي:

أ. **الابتزاز الجنسي(الأخلاقي):** انتشر نوع من أنواع جرائم الابتزاز الإلكتروني يعتمد على "الرغبات الجنسية" نتيجة التطور التقني الذي ساعد على انتشار جرائم الابتزاز الإلكتروني عبر تقنيات الاتصال

المتطورة، وما أتاحتها الشبكة العنكبوتية (الإنترنت) من قدرة على الاتصال والتواصل عبر آلاف الأميال، حيث يعتبر من أكثر أنواع الابتزاز الإلكتروني شيوعاً، إذ يطلب المبتز فيه من الضحية إشباع رغباته الجنسية، ذلك من خلال التهديد بفضح أمرها وتحديدًا إن كانت تتصف بضعف شخصيتها وضعف إرادتها وعدم قدرتها على حماية نفسها، من ثم تصعيد نغمة التهديد بالفضيحة بين أهلها وأصدقائها من خلال نشر صور إباحية لها على شبكة الإنترنت، بهدف ممارسة الجنس أو الفحشاء معها أو مع غيرها من الأصدقاء (دقيش، 2010: 42).

يطلق أيضاً على الابتزاز الجنسي مفهوم الابتزاز الأخلاقي، وهذا ما أكدته (الشرطة الفلسطينية، 2019) من خلال بيان أصدرته إدارة وحدة العلاقات العامة والإعلام بالشرطة بأنه وصل لها شكوى من إحدى المواطنات في مدينة الخليل مفادها بأنها تتلقى تهديدات وابتزازاً أخلاقياً (جنسياً) من خلال موقع الفيس بوك مقابل عدم نشر صورها وفضحها، حيث قامت وحدة الجرائم الإلكترونية بتلقي الشكوى والعمل عليها مباشرة، من ثم القبض على الجاني (المبتز) وتحريز الهاتف الذكي الذي يستخدمه أثناء ارتكابه جريمة الابتزاز حيث يحتوي على صور ومعلومات مقدمة الشكوى.

ب. الابتزاز العاطفي: يقوم المبتز في هذا النوع من الابتزاز الإلكتروني في اختيار ضحيته التي تمتاز بتدني مستوى الذكاء العاطفي لديها أي "لا تتمتع بمكونات الذكاء العاطفي"، ليقوم بإنشاء علاقة عاطفية بينهم تعمل على إرضاء الضحية في البداية، من ثم يستغل المبتز (الجاني) حب الآخرين له أو تعاطفهم معه، حيث يستخدم الحيل والدهاء لتوجيههم وجهة معينة أو جعلهم يتصرفون تصرفاً كأنهم مخطئون بحقه، ذلك من خلال كلام أو موقف يفتعله ليسبب للضحية إحساساً بالخجل أو الخطأ أو ليحملها المسؤولية، إذ يحاول تحقيق سيطرة عاطفية ونفسية على الضحية، لجعلها تشعر بأنها تدين له ومذنبة في حقه، من ثم يقوم بابتزازها عاطفياً وطلب غايته منها، فتحاول إرضاءه حتى لا تخسر العلاقة العاطفية فيما بينهم (حمد، 2009: 15).

ج. الابتزاز المادي: الهدف الأساسي لهذا النوع من الابتزاز هو "مادي بحت"، حيث يتبع الجاني العديد من الطرق للحصول على مبتغاه المادي، ولعل أهم هذه الطرق الابتزاز الجنسي، فقد يطلب المبتز من الضحية أموالاً مقابل عدم الفضيحة، إذ يتضمن الابتزاز المادي التهديد من خلال طلب مبالغ مادية من الضحية وإجبارها على دفعها بشكل مستمر حتى لا يقوم المبتز بنشر صور أو

محدثات أو بيانات خاصة بالضحية على شبكة الإنترنت، قد يستمر هذا الابتزاز سنوات عدة طالما أن الضحية تقوم بدفع المال بشكل مستمر، لكن عندما تقوم برفض دفع الأموال يبدأ المبتز في استخدام الحيل للضغط على ضحيته وإرغامها على توفير الدفعات المطلوبة منها (السعدون، 2008:23).

مما سبق نجد أنّ الدافع المادي هو السبب الرئيسي لارتكاب بعض جرائم الابتزاز الإلكتروني، حيث ذكر بيان من (الشرطة الفلسطينية، 2019) من خلال إدارة وحدة العلاقات العامة والإعلام بالشرطة بأنّ سيدة من الخليل توجهت لوحدة الجرائم الإلكترونية بشكوى ضدّ مجهول يقوم بابتزازها من خلال طلب مبلغ مالي مقابل عدم التشهير بها ونشر صورها، في البداية استجابت السيدة له وقدمت له المبلغ المطلوب، لكن لم يتوقف عن ابتزازها وبدأ في طلب المزيد، لم تسطع الضحية السيطرة على مجريات عملية الابتزاز فتوجهت لوحدة مكافحة الجرائم الإلكترونية لطلب يدّ العون، حيث باشرت وحدة الجرائم الإلكترونية التحقيق في الواقعة والاستعانة بالأدلة الإلكترونية للقبض على الجاني، تمكنت من الوصول إليه والقبض عليه وتحريز الهاتف الذكي الذي يستخدمه في عملية الابتزاز وأخذ الإجراءات القانونية بحقه.

د. الابتزاز السياسي: ينشأ هذا النوع من الابتزاز نتيجة الاختلافات السياسية أو وجود دولة محتلة وأكبر دليل على ذلك دولة فلسطين المحتلة التي تعاني من الابتزاز السياسي من قبل الاحتلال الإسرائيلي لتحقيق أهداف وغايات سياسية، اقتصادية، اجتماعية (العميري، 2004:31)، نلاحظ أيضاً تنوع الأحزاب السياسية المختلفة في دولة فلسطين المحتلة، إذ نشأت نتيجة تواجد الاحتلال الإسرائيلي الذي زرع الفتنة فيما بينهم لجعلهم في صراع دائم ومستمر، مما جعل بعض الأفراد في هذه الأحزاب يستخدمون الابتزاز السياسي لتحقيق أهداف معينة، بالإضافة إلى استخدام الاحتلال الإسرائيلي لأساليب متنوعة للابتزاز السياسي الذي أصبح حديثاً يتم من خلال الشبكة العنكبوتية لإسقاط الشباب والضغط على القيادات السياسية في دولة فلسطين المحتلة، ذلك بسبب امتلاكه إمكانيات تكنولوجية عالية التقنية تمكنه من التجسس على جميع من يستخدم الإنترنت في فلسطين، والدليل على ذلك قيام دولة الاحتلال بتأسيس وحدة (8200) لمراقبة ومتابعة الشعب الفلسطيني ومعرفة اهتماماتهم ورغباتهم حيث يعتبر نسبة الأفراد الذين يستخدمون موقع الفيس بوك (87%) من إجمالي المواطنين مقارنة بالعام (2016) (النعامي، 2017).

وأكد (غفري، 2015) أن هناك محاولات متنوعة بالسرّ والعلن لأجهزة الشابك، تستهدف إسقاط غزة عبر موقع الفيس بوك"، حيث قام الشابك أي جهاز المخابرات للاحتلال الإسرائيلي باستخدام العديد من الوسائل والطرق لإسقاط الشباب الفلسطيني من ضمنها استخدام مواقع التواصل الاجتماعي وأهمها موقع الفيس بوك لابتنزاهم جنسيًا وماديًا وتهديدهم وإرغامهم على تنفيذ غايتهم خاصة التجسس على من حولهم، ذلك من خلال حسابات وهمية لفتيات تقدم الهوى أو من خلال إعلانات موجهة لفئة ومنطقة معينة تقوم بتقديم إغراءات للشباب الفلسطيني، أيضا من خلال صفحات بأسماء ضباط ومجندين في جهاز الشابك وقيادات متحدثة إعلاميًا عن جيش الاحتلال مثل أفخاي أدري، حيث يتم استدراجهم من خلال الوسائل السابقة وتتبع عنوان ال (IP) لمعرفة المنطقة الجغرافية المتواجدين بها من ثم تحقيق غايتهم وأهدافهم.

5.2.2 أركان جرائم الابتزاز الإلكتروني:

إنّ جرائم الابتزاز الإلكتروني كغيرها من الجرائم الأخرى لا يمكن اعتبارها جريمة إلا إذا توافرت فيها الأركان الأساسية للجريمة التي تتمحور في:

• **الركن المادي:** يعني السلوك أو النشاط المادي الذي يمثل في جريمة الابتزاز الإلكتروني البيئة رقمية والاتصال بالإنترنت، على سبيل المثال يقوم الجاني بإحضار جهاز الحاسب الآلي حتى يقوم بارتكاب الجريمة، من ثم يحمل على جهاز الحاسب الآلي برامج اختراق أو يقوم بإعدادها، من ثم يقوم بالبحث عن ضحيته المناسبة للإيقاع بها، إذ يتمثل الركن المادي في السلوك أو النشاط الذي يستخدمه الجاني في الاعتداء والاختراق على جهاز الضحية، من خلال الدخول والبقاء غير المشروع في الحاسب الآلي، من ثم الاعتداء على بيانات الضحية بعدة طرق قد تكون محوها أو سرقتها أو استخدامها بطرق غير مشروعة لتخدم أهدافه (خطوة، 2007: 226).

• **الركن القانوني:** نعني بالركن القانوني توافر نصّ قانوني أو شرعي يجرم ويعاقب الجاني حين قيامه بالفعل الإجرامي، لكن يشترط أن يكون الفعل الإجرامي واضحا ومعرفا بالقانون ليتم المحاسبة على هذا الفعل استنادا للقانون، ذلك للحفاظ على أمن المجتمع وإقامة العدل ما بين المواطنين، من ثم الحفاظ على نسيج التركيب المجتمعي (عودة، 2008: 70).

• **الركن المعنوي:** نعني بالركن المعنوي أي شخصية الجاني وحالته النفسية، حيث تمّ التوضيح سابقاً عن علاقة الذكاء العاطفيّ بالسمات الشخصية للضحية وكيف تؤدي إلى وقوع الفرد كضحية لدى الجاني، إضافة إلى ذلك العلاقة المكتملة التي تربط بين ماديّات الجريمة المتمثلة بالركن المادي وشخصية الجاني المتمثلة بالركن المعنوي، حيث يقوم الجاني في مختلف الاعتداءات والاختراقات المساس بالأنظمة المعلوماتية والبيانية في جهاز الضحية، لينتج صورة القصد الجنائي المعروف بالقانون من خلال الدخول و التجول والبقاء داخل نظام المعالجة الآلية لجهاز الضحية (عبد الحكيم، 2015: 203).

6.2.2 أسباب ارتكاب جرائم الابتزاز الإلكتروني:

هناك اختلاف بين مرتكبي جرائم الابتزاز الإلكترونيّ الحديثة عن مرتكبي الجرائم التقليدية، يرجع ذلك الاختلاف إلى عدة عوامل منها السن والجنس والمستوى التعليمي، إضافة إلى اختلاف الأسباب أو الأهداف أو الدوافع الداخلية التي قد تدفعهم لارتكاب الجريمة، حيث تُعدّ بعض العوامل كالمحبة والبغضاء والانتقام وكسب المال هي المحرك التي تدفع بعض الأفراد لارتكاب الفعل الإجرامي لتحقيق غاية معينة (الغافري، 2014).

هناك العديد من الأسباب التي تدفع الجاني لارتكاب جرائم الابتزاز الإلكترونيّ، لعل من أهمها ما يلي:

1- **العامل الماديّ (المالي):** يعتبر العامل المادي من أهم تلك الأسباب التي تدفع الجاني وتحركه نحو ارتكاب جريمة الابتزاز الإلكترونيّ للحصول على مكاسب وأرباح مادية بالطريقة السهلة، لذا يقوم الجاني بالاعتداء واختراق جهاز الضحية والسيطرة على البيانات والمعلومات، ذلك يأتي نتيجة ضعف الوازع والرداع الديني والفقير والبطالة (كرسوع، 2016).

2- **العامل القانوني:** المتمثل في استغلال التطور التكنولوجي لارتكاب جرائم الابتزاز الإلكترونيّ التي تتمّ من خلال استخدام الشبكة العنكبوتية (الإنترنت)، التي سهلت عملية التواصل والاتصال بين الأفراد دون حدود جغرافية ومكانية، وصعوبة ملاحقة مرتكبيها خاصة في ما بعض الدول التي أغفلت سنّ قانون رادع.

3- العامل الاجتماعي: المتمثل في استغلال الآخرين من خلال نقاط الضعف الخاصة في حياتهم كالتفكك الأسري، أو الحاجة إلى العاطفة، أو ضعف الرادع الديني، إضافة إلى رفاق السوء التي قد تدفعه لارتكاب هذا النوع من الجرائم للتباهي فيما بينهم (المناعسة، والزعبي، 2014: 94).

4- العامل الشخصي (للجاني): يوجد العديد من الأسباب التي قد تدفع الجاني لارتكاب فعلته لعل من أهمها الانتقام للحصول على الشهرة في بعض الأحيان، أو إلحاق الضرر بفرد أو مجموعة أو جهات، وفي بعض الأحيان يكون الدافع الطمع بعلاقات غير شرعية (كرسوع، 2016).

كما ويُعتبر تحقيق الأرباح المادية والمكاسب المادية بطريقة سهلة وغير عنيفة من أهم الأسباب التي تؤدي إلى ممارسة جريمة الابتزاز الإلكتروني، حيث يقوم الجاني بتهديد الضحية لإجبارها على الخضوع له وإعطائه الأموال التي قد يطلبها لمرة واحدة، لكن قد يقوم الجاني بالابتزاز بشكل دوري ومستمر عند تجاوب وتعاون الضحية معه، فيقوم بتهديدها بأنه سيقوم بالتشهير بها وفضحها من خلال نشر الصور أو البيانات أو المحادثات أو الفيديو الخاص بها، لذا قد يقوم بمحاولة إخضاعها وإجبارها على إرسال معلومات خاصة بها لإشباع رغباته الجنسية، لكن قد يختلف هدف الجاني وفقا لميوله وأهدافه من ارتكاب جريمته فمنهم يقوم بارتكاب جريمته للحصول على الشهرة في مجتمعه، خاصة بين أقرانهم للتباهي في قدرتهم وذكائهم في التعامل مع وسائل التواصل وبرامج الاختراق والتكبير والاعتداء، إضافة إلى مدى تأثير التفكك الأسري والاجتماعي لدى الجاني الذي قد ينتج عنه فراغ عاطفي لديه، مما يولد الرغبة في سدّ هذا الفراغ من خلال العلاقات العاطفية بواسطة مواقع التواصل الاجتماعي، لكن عند شعوره بالتهديد أو خسارة هذه العلاقات قد يلجأ إلى جريمة الابتزاز الإلكتروني لكي يحافظ عليها، مما يجعله يلحق الأذى بنفسه وبالأخرين.

7.2.2 خصائص جرائم الابتزاز الإلكتروني:

تتميز جرائم الابتزاز الإلكتروني من خلال مفهوم الجريمة بخصائص تميزها عن الجرائم الأخرى، لعل من أهم تلك الخصائص ما يلي:

• جريمة عابرة للدول، "من أهم ما يميز جرائم الابتزاز الإلكتروني بأنها لا تعرف الحدود الجغرافية والمكانية، حيث بالإمكان أن تقع بين عدة دول دون معرفة الجاني، فمع انتشار الشبكة العنكبونية (الإنترنت) في كل منزل ومكان عمل تقريبا، وانتشار الأجهزة الذكية لدى الغالبية العظمى

من الأفراد أصبح بالإمكان ربط عدد لا محدود له من الأفراد عبر تلك الشبكة العنكبوتية حول العالم، حيث سهلت تبادل المعلومات بين الدول وبين الأفراد، مما أسهم في نشوء نوع جديد من الجرائم تُسمى الجرائم الإلكترونية التي من أنواعها جرائم الابتزاز الإلكتروني، حيث يمكن أن ترتكب جريمة الابتزاز الإلكتروني في عدة دول تبعد عن بعضها مسافات قد تمتد آلاف الأميال، أيضا من الممكن أن يكون الجاني في دولة والمجني عليه في دولة أخرى، وقد يكون الدليل في دولة ثالثة، فالسهولة في حركة المعلومات والبيانات عبر أنظمة التقنيّة الحديثة والأجهزة الذكية مستخدمين الشبكة العنكبوتية جعل إمكانية ارتكاب الجريمة عبر حاسب آلي موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى ذلك من خلال مجتمع الشبكة العنكبوتية (الإنترنت)، كما أن ضرر هذه الجرائم يتعدى إلى أكثر من دولة ليكون الضرر أكبر من خلال إرسال فيروس للاختراق والتجسس مما قد يصيب أكثر من جهاز في عدة دول تبعد عن بعضها مسافات طويلة، مما نتج عن طبيعتها الإجرامية العديد من المشاكل حول تحديد الدول ذات الاختصاص القضائيّ بهذه الجريمة، كذلك حول القانون الواجب تطبيقه إضافة إلى الإشكاليات المتعلقة بإجراءات الملاحقة القضائية وإجراءات الإثبات وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود التي تجعل إمكانية التحري والتنسيق أمرا صعبا وشاقا ومكلفا للجهات الأمنية والقضائية" (المناعسة، والزعبي، 2014: 95).

• **مغرية لذوي النشاط الإجرامي، تُعدّ جرائم الابتزاز الإلكتروني من الجرائم الناعمة التي لا تحتاج إلى أسلحة لتنفيذها، حيث لا تحتاج ذهاب الجاني مسافات أو الخروج ليلا أو حتى استخدام وسيلة نقل للانتقال لمكان الضحية، بل تحتاج فقط إلى ضغطت زر لارتكاب جريمته دون الحاجة إلى الذهاب لمكان الجريمة أو بذل مجهود جسدي، لذلك تُعدّ جريمة مرغوبة لذوي النشاط الإجرامي لقلّة المخاطر والمشقة فيها، كما تُعدّ جريمة ذات مردود مالي كبير بالطريقة السهلة فهي تحقق أرباحا أكثر من الأرباح التي تحققها الجرائم التقليدية سواء بالسرقة أو توظيف الأموال كما يحدث عندما يتمّ ابتزاز دول معينة أو عند ابتزاز الشركات والمؤسسات الكبرى أو ابتزاز أفراد (أبكر، 1999: 47).**

• **سهولة الارتكاب، تُعدّ جرائم الابتزاز الإلكتروني من الجرائم الناعمة التي لا تحتاج إلى عنف أو ضرب أو تكسير ولا تحتاج إلى أي مجهود عضلي بل يمكن ارتكابها قبل الجاني بضغط زر وهو في بيته ويحصل على ما يريد، فهي جريمة تعتمد على الفكر والذكاء لا العنف، من خلال التقنيات الحديثة التي تمكنه من ارتكاب جريمته بأسرع وقت وجهد ممكن، لذا تُعدّ جرائم الابتزاز الإلكتروني**

جرائم هادئة بطبيعتها لان كل ما يحتاجه الجاني هو معرفة بكيفية التعامل مع جهاز الحاسب الآلي بمستوى فني وتقني يستغل فيها خبرته ومهارته داخل شبكة عنكبوتية (الإنترنت) مما يؤدي لارتكابه الجريمة سواء بالاختراق والاعتداء والتجسس أو بإقامة العلاقات الغرامية (العاطفية) أو الابتزاز، فهي جريمة لطيفة وناعمة كونها لا تترك آثار عنف أو دماء وإنما اختراق واعتداء على أرقام وبيانات يتم الحصول عليها بعمل تقني وفني (الكعبي، 2009:29).

• **صعوبة الإثبات، تُعدّ جريمة الابتزاز الإلكترونيّ جريمة صعبة الإثبات** لأنه يتم فيها استخدام وسائل تقنية حديثة ومعقدة لا يمتلك كافة الأفراد قدرة على فهمها واستغلالها، حيث تمتاز بسهولة مسح الأدلة التي تدل على مكان وهوية الجاني والتلاعب فيها، حيث أنها في الغالب لا تترك اثر مادي يمكن فحصه لأنها جرائم خفية قد لا يلاحظها الضحية رغم أنها تقع أثناء وجودها على الشبكة العنكبوتية (الإنترنت) بسبب قدرة الجاني على تنفيذ جريمته بدقة عالية، ويستفيد الجناة من هذا النوع من الجرائم من خلال مواقع القرصنة "الهacker" بحيث يتم التواصل مع بعضهم البعض لتبادل المعارف والخبرات في مجال القرصنة والتجسس والأفكار الإجرامية المتنوعة مما يساهم في ارتكاب المزيد من الجرائم، وجريمة الابتزاز الإلكترونيّ بحكم ارتباطها بالشبكة العنكبوتية (الإنترنت) وبرامجها والتطور السريع فيها فهي أسرع تطور من التشريعات والقوانين التي تنص عليها الجهات التشريعية لمواجهتها بسبب التباين والاختلاف الكبير بين سرعة التطور التقني والتفاعل السريع بين مرتكبي الجريمة لتبادل الأفكار وبين التعقيدات التي تمرّ عليها التشريعات والبيروقراطية الحكومية من أجل سنّ القوانين لمواجهة جريمة الابتزاز الإلكترونيّ، إضافة إلى ضعف التأهيل للجهات الأمنية وتعاملهم مع هذا النوع من الجرائم في بعض الدول مما نتج عنها قلة معرفتهم بالأمور الفنية والتقنية للحاسب الآلي، وكيفية التعامل معه كمسرح افتراضي للجريمة ، كما أنّها لا تزال محل جدل داخل القضاء في تقبل الأدلة المادية الموجودة داخل العالم الافتراضيّ بالحاسب الآلي وإمكانية إثباتها كدليل ماديّ معتبر لدى القضاء في بعض الدول، حيث تُعدّ أدلة الإدانة الإلكترونية ذات نوعية متميزة عن غيرها من الأدلة مثل سجلات الحاسب الآليّ أو معلومات الدخول التي قد تثير العديد من المشاكل والشك لدى القضاة ومصداقية تلك الأدلة، حيث تحتاج هذا الجرائم إلى وقت طويل من التنسيق والبحث للوصول إلى دليل، ومن الممكن ألاّ يتمّ إيجاد أي دليل إدانة (باطلي، 2015: 28-32).

نلاحظ ممّا سبق بأن الجرائم الإلكترونية لديها العديد من الأنواع من أهمها جرائم الابتزاز الإلكتروني، تتمتع بخاصية حرية الحدود بسبب استخدامها الشبكة العنكبوتية (الإنترنت) التي جعلت العالم قرية صغيرة وسهلت عملية الاتصال والتواصل دون قيود أو حدود، لكنّ هذه التسهيلات حملت في طياتها بعض المخاطر والثغرات التي قام باستغلالها ضعاف النفوس، ليظهروا أنواعا جديدة من الجرائم لكن بوسيلة جديدة تتمثل في الوسائل التقنية ومواقع التواصل الاجتماعي المختلفة، حيث أصبحت تستخدم من النسبة الأكبر من الأفراد والمؤسسات والجهات الحكومية في المجتمعات، إذ يتنوع أهداف وغايات استخدامها، ممّا قد ينجم عنها بعض المحاولات لارتكاب جرائم إلكترونية من خلال اختراق وسرقة المعلومات الخاصة بالحاسبات الآلية والمواقع حتى لو كانت في دولة أخرى، حيث تُعدّ جرائم الابتزاز الإلكتروني مغرية لمن تتوفر لديه عدة عناصر مهمة منها الإرادة الإجرامية أي رغبته في الحصول على مردود مادي أو غير مادي بطرق غير مشروعة، إضافة إلى اختياره ضحية مناسبة لتحقيق غايته، واستغلال عدم وجود رقابة على الشبكة العنكبوتية للقيام بجريمة الابتزاز الإلكتروني حيث تتميز بقلّة المجهود والمشقة عند القيام بها ممّا جعلها مغرية لضعاف النفوس، فهي جرائم هادئة قد يرتكبها الجاني دون معرفة من حوله بأنّه قام بها أو يشعرون به، ممّا ولد العديد من الصعوبات في تحديدها وأثباتها نتيجة التطور الهائل والمستمر في التقنيات والفنيات الحديثة، حيث بالإمكان أن تحدث عملية سرقة لمعلوماتك وبياناتك الشخصية دون أن تشعر بذلك، إضافة إلى مسح الأدلة التي تفيد بارتكاب الجاني هذه الجريمة نحوك، لذا نجد الأجهزة المختصة بتطوير مستمر لتقنياتها وطاقتها لمواكبة التطورات التقنية والفنية المتجددة باستمرار للكشف عن هذه الجرائم.

8.2.2 آثار جرائم الابتزاز الإلكتروني:

يوجد العديد من الآثار السلبية لجريمة الابتزاز الإلكتروني تحديدا على الضحية وأسرتها وعلى المجتمع معاً، لعل من أهمها:

1- الآثار السلبية على الفرد (الضحية)، انتشار الأمراض النفسية والجنسية لدى الضحايا، وانتشار الفاحشة (الجنس)، اضطرابات في النوم والأكل، والعزلة والوحدة، والانتحار، وفقدان الضحية ثقافتها بنفسها، ممّا يجعلها شخصية مضطربة وغير سوية، وقد تصاب الضحية بالاكتئاب، والانهيار

العصبي، وتصبح الضحية تعاني من الشك والكوابيس المزعجة، وإهمال الواجبات الاجتماعية، إضافة إلى التغيب عن العمل أو الدراسة، ولا تستطيع الضحية التعامل مع الآخرين (مركز باحثات لدراسات المرأة، 2011: 23)

2- الآثار السلبية على أسرة الضحية والمجتمع: تفكك أسري ومجتمعي، القتل للضحايا في بعض الأحيان خوفاً من وصمة العار التي قد تلحق بالأسرة، وانتهاك المحارم والمحرمات، المشاكل والخلافات ما بين عائلة الضحية وعائلة الجاني، مما ينتج زعزعة الطمأنينة والأمن المجتمعي (نبيه، 2008: 39).

مما سبق يتضح أنّ هناك العديد من الآثار السلبية التي تنتج عن جريمة الابتزاز الإلكتروني، فهي تقلل من ثقة الضحية بنفسها وإصابتها بأمراض نفسية أو حتى انهيار عصبي، ذلك نتيجة تدني مستوى الذكاء العاطفي لديها حين مواجهتها جريمة الابتزاز الإلكتروني، وأما فيما يخص آثارها على أسرة الضحية، ففي الغالب تقوم الأسرة بالتخلص من الضحية خوفاً من وصمة العار من خلال القتل مما يسبب تفككا أسرياً وانعدام الأمن الداخلي بالأسرة، إضافة لنشوء العديد من الخلافات المتعددة والمستمرة، وهذا كلّه - بالتأكيد- سيؤثر على المجتمع الذي يتواجدون فيه مما يؤدي إلى زعزعة الأمن المجتمعي وعدم الشعور بالأمن والأمان أساس الحياة واستمرارها.

9.2.2 سمات وصفات الضحايا والجناة في جرائم الابتزاز الإلكتروني:

سوف يتم الحديث عن أهم سمات وصفات الأفراد الذين يرتكبون جرائم الابتزاز الإلكتروني والأفراد الذين يتعرضون لهذه الجرائم، في البداية سوف يتم الحديث عن طبيعة الأشخاص الذين يتعرضون للابتزاز الإلكتروني وأهم سماتهم، ثم الانتقال للحديث عن سمات الجناة، فالحديث عن ضحايا جرائم الابتزاز الإلكتروني يشمل التركيز على وسيلة ارتكابها، كون التقنيات التكنولوجية ووسائل التواصل شملت مناحي الحياة كافة، لذا تعدّ جريمة الابتزاز الإلكتروني من ضمن الجرائم الإلكترونية (السعدان والشمري، 2010: 14-15).

تتمثل سمات وصفات كلّ من الضحايا والجناة في الآتي:

1- سمات وصفات الضحايا، يعدّ أكثر الأشخاص عرضة لجرائم الابتزاز الإلكتروني هم من كبار السنّ وصغار السن، ثم النساء اللواتي يقضين أوقات فراغهنّ خارج المنزل، والنساء اللواتي

يستخدمنّ المواصلات العامة والشباب والمراهقين من كلا الجنسين الذين يعانون من بعض المشاكل الأسرية أو التعليمية، والشباب والمراهقين الذين لا يجدون من يستمع إليهم أو يحتويهم، والشباب والمراهقين الذين كانوا ضحايا للخلافات الزوجية والانفصال لذويهم، والشباب والمراهقين الذين يتأثرون بأقرانهم، والأفراد الذين يمتلكون المال والسلطة والجمال والمعلومات، وأفراد من أقليات عرقية، وأفراد من أسر ومجتمعات فقيرة يتصفون بشكل عام بوجود العديد من المشاكل (الأسرية، والاجتماعية، والمادية)، وأفراد لا يقدرّون على مواجهة الواقع ويهربون منه، وأفراد يخافون التعامل مع الآخرين، وأفراد لديهم استعداد للفشل، وأفراد اعتمدين على غيرهم، وأفراد فارغين من داخلهم ليس لديهم أهداف لحياتهم، وأفراد سريع التآثر بالآخرين، وأفراد يعانون من عدم المقدرة على تميّز الأمور (العمر، 2009: 134؛ العمر، 2012: 223-224؛ العمر 2015: 223؛ الصالح، 2011: 119).

2- سمات وصفات الجناة، أمّا فيما يتعلق بسمات وصفات جناة جرائم الابتزاز الإلكتروني، فقد وضّح (طالب، 2007: 146-151؛ الصالح، 2011: 118؛ دسوقي، 2011: 200)، أنّهم ينتمون إلى الشخصية السيكوباتية (شخصية مصابة بمرض عصابي خطير من مؤشرات القلق الشديد، الغيرة الشديدة غير المبررة، الانفعال المفرط)، يتلذذون في إيذاء الآخرين وتعذيبهم، لديهم دافعية قوية لتحقيق الرغبة وإشباع الملذات دون التفكير بالعواقب، ولديهم حب السيطرة والتملك، وسرعة الانفعال والتهور، والأنانية والإفراط في حب الذات، وقسوة القلب دون الإحساس بالذنب، وأعمارهم ما بين 18-45 سنة، لديهم معرفة قوية بالتقنيات التكنولوجية الحديثة، ومعظمهم متعلمون، والثقة الزائدة بالنفس، ومستوى عالٍ من الذكاء.

نلاحظ ممّا سبق أنّ السمات والعوامل التي تميّز كلاً من الضحايا والجناة في جرائم الابتزاز الإلكتروني، إذ إنّ الذي لا يتمتع بمستوى ذكاء عاطفي عالي من الممكن أن يكون ضحية لهذه الجرائم، ذلك لأنها لا تتمتع في مكونات الذكاء العاطفي من وعي بذاتها ولا تستطيع مواجهة واقعها الذي تعيش فيه وتفضل الهروب منه، والخوف مسيطر على كافة حياتها، ليس لديها دافعية للإنجاز والتطوير من نفسها، حيث لا تقوم بالتخطيط لحياتها ولا تضع لها الأهداف، لذا نراها تتأثر بالآخرين بسهولة، بالإضافة إلى ذلك تعاني الضحية من عدم مقدرة على تمييز مشاعرها وانفعالاتها في المواقف ولا تمييز مشاعر وانفعالات الآخرين، ممّا يجعلها فريسة سهلة المنال لجاني يتمتع بمستوى ذكاء عالٍ، ويتميز بالثقة بالنفس ليقوم بإخضاع الضحية، ويتلذذ في تهديدها وإكراها على تنفيذ طلباته ورغباته.

10.2.2 واقع الجرائم الإلكترونية في فلسطين:

تعاني دولة فلسطين من إشكاليات قانونية في المجال الجنائي والقضائي نتيجة ازدواجية قوانين العقوبات المطبقة فيها بين الضفة الغربية وقطاع غزة وقدمها، ففي الضفة الغربية يطبق قانون العقوبات الأردني لعام (1960) ولا يشمل أية تعديلات أجريت عليه بعد عام (1967)، وفي قطاع غزة يطبق فيها قانون العقوبات الفلسطيني "الانتدائي" رقم (74) لسنة (1936)، على الرغم من انتخاب مجلس تشريعي فلسطيني بعد إنشاء السلطة الفلسطينية في عام (1994)، إلا أن هذا المجلس الذي أعيد انتخابه في العام (2006) لم ينجح في إقرار قانون عقوبات موحد يواكب تطورات العصر، فاكتمل المجلس التشريعي بإقرار مشروع قانون العقوبات بتاريخ (2003/4/14)، حيث خلت قوانين العقوبات القديمة المطبقة في كل من الضفة الغربية وقطاع غزة من نصوص صريحة لتجريم الجرائم الإلكترونية، ذلك بسبب قدم القانون الذي تمّ وضعه قبل إدخال خدمة الإنترنت وأجهزة الحاسوب والهاتف وغيرها، القائم على البند رقم (15) الذي ينص على "عدم وجود عقوبة دون نص قانوني"، لذا نتجت حاجة ملحة لهذه القوانين أصدرت فلسطين بعض القوانين الخاصة، التي أشارت من خلالها إلى بعض الجرائم الإلكترونية ضمن نصوص غير واضحة، لمحاولة التخفيف من الضغوط المجتمعية والجهات الرسمية التي تطالب الجهات المختصة بملاحقة الجرائم ومعاقبه مرتكبيها، فاستندت إليها الوحدة العامة واستخدمتها في المحاكم، ويقف على رأس هذه القوانين، القرار بقانون رقم (15) لعام (2009) بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات، والقانون رقم (3) لعام (1996) بشأن الاتصالات السلكية واللاسلكية (الريس وآخرون: 2003) (جريدة الوقائع الفلسطينية، 1996، ص7).

لاحقا في عام (2010) تمّ عمل مسودة لتعديل قانون العقوبات بإشراف وزارة العدل الفلسطينية، لكن لم يتمّ إصداره نتيجة خلوه من عقوبات الإعدام والأشغال الشاقة للجنّة، حيث لم يتمّ مراعاة الجرائم الحديثة، ومنها الجرائم الإلكترونية الناشئة بسبب تطور التقنيات التكنولوجية، حيث أخذت بالازدياد بشكل سريع، ممّا جعل هناك حاجة ماسة إلى رادع قانوني، فتمّ إعداد مقترح من خلال ديوان الفتوى والتشريع لمشروع قانون الإنترنت والمعلوماتية المكون من (86) مادة (الشامي، 2010).

ولكن، بعد ازدياد الجرائم الإلكترونية وامتداد أثرها السلبي على كافة المجتمع، تمّ دراسة أطروحة قانون الجرائم الإلكترونية، حيث رأت الحكومة الفلسطينية بأنه عليها المصادقة على هذه الأطروحة

لتنظيم المواقع الإلكترونية والإعلامية ومواقع التواصل الاجتماعي، وفرض عقوبات على من يخلّ بالسلوك العام أو يحرّض من خلال هذه المواقع، جاء هذا القرار ليعالج الجرائم الإلكترونية التي ارتفعت معدلاتها في الأراضي الفلسطينية خلال السنوات الأخيرة كما تمّ الحديث عنه سابقاً، ففي عام (2015) بلغ عدد البلاغات الرسمية عن تلك الجرائم (502)، وفي العام (2016) بلغ عدد الجرائم (1327)، وارتفعت في عام (2016) إلى (26.6%) (2025) قضية، بينما في (2018) سُجّل (2568) قضية بنسبة (26.6%) (جهاز الشرطة الفلسطينية، 2019).

حيث أصدر(الجهاز المركزي للإحصاء الفلسطيني، 2017) إحصائيات تفيد بأنّ نسبة الجرائم الإلكترونية بلغت (30%) من نسبة الجرائم المرتكبة في فلسطين، وبعد تزايد النسبة قام رئيس دولة فلسطين محمود عباس بموجب الصلاحيات الدستورية الممنوحة بإصدار مجموعة من القوانين المستحدثة التي تخدم التطور التكنولوجي والتقني نتيجة الحاجة الملحة لها، حيث تمّ إصدار قانون رادع للجرائم الإلكترونية في دولة فلسطين احتوى هذا القانون على (61) مادة قانونية خاصة بالجرائم الإلكترونية بتاريخ (2017/06/20) للمزيد من التفاصيل انظر/ي ملحق رقم (6) (جريدة الوقائع الفلسطينية، 2017: 31)، لكنّ هذا القانون تضمن مواد تتعارض مع الحريات كحرية التعبير والرأي، لذا تمّ إعادة تعديله بناء على الرفض والشجب من قبل عامة الناس خاصة الصحفيين لأنّه يحدّ من حريتهم، وصدر التعديل لقانون الجرائم الإلكترونية رقم (10) في عام (2018) للمزيد من التفاصيل حول المذكرة القانونية التي تحدد أسباب تعديل القانون انظر/ي الملحق رقم (8) (الهيئة المستقلة لحقوق الإنسان، 2018).

وفي عام (2017) تمّ إصدار قانون الجرائم الإلكترونية رقمه (16)، واحتوى هذا القانون على (61) مادة قانونية خاصة بالجرائم الإلكترونية، ليكون رادعاً للجناة الذين يستخدمون الحاسب الآلي والأجهزة الإلكترونية الحديثة منها (الهواتف الذكية، والحاسب الآلي المحمول، والجهاز اللوحي) للقيام بابتزاز الأفراد من خلال الشبكة العنكبوتية (الإنترنت) مستغلين ضعف الجانب الأمني لأفراد المجتمع في هذا الخصوص، وكون الأفراد ليس لديهم معرفة عالية بالتطورات التكنولوجية المتتابعة والمتطورة، لكن عمل هذا القانون أيضاً على التدخل بالحريات الفردية (الشخصية) والتي منها حرية التعبير عن الرأي والحق في الخصوصية وفقاً للجهات الإعلامية والحقوقية في فلسطين، من خلال المناقشات مع كافة الجهات المختصة تمّ إصدار تعديل على القانون ليتناسب مع الوضع الراهن بتاريخ

(2018/04/29)، للمزيد من المعلومات يرجى الاطلاع على المذكرة القانونية حول قانون رقم (10) لسنة (2018) بشأن الجرائم الإلكترونية انظر/ي الملحق رقم (7)، لذا تمّ إعادة تعديله بناء على الرفض والشجب من قبل عامة الناس خاصة الصحفيين لأنّه يحد من حريتهم، صدر التعديل لقانون الجرائم الإلكترونية رقم (10) في عام (2018) للمزيد من التفاصيل حول المذكرة القانونية التي تحدد أسباب تعديل القانون انظر/ي الملحق رقم (8) (الهيئة المستقلة لحقوق الإنسان، 2018).

لذا عند الحديث عن واقع الجرائم الإلكترونية وجرائم الابتزاز الإلكتروني والإحصائيات المبيّنة لها في فلسطين، علينا أن نشير أيضا إلى مدى تزايد استخدام الإنترنت خلال السنوات السابقة وعلاقته بتزايدها، حيث تشير الإحصاءات السابقة الصادرة عن جهاز الشرطة الفلسطينية بأنّ "هناك زيادة لاستخدام الإنترنت في فلسطين، نتيجة لهذا الاستخدام والانتشار الواسع نتج عنها تزايد في الجرائم الإلكترونية من ضمنها جريمة الابتزاز الإلكتروني، حيث سجلت الشرطة الفلسطينية في العام (2015) (502) قضية، وفي عام (2017) (1327) قضية، بينما في عام (2018) سُجّل (2568) قضية، نلاحظ الزيادة المستمرة لعدد القضايا المسجلة مقارنة بالسنوات السابقة"، إنّ ما سبق من نسب يوضح لنا الزيادة في عدد القضايا المسجلة، وقد لا يكون السبب ضعفا في تطبيق القانون الخاص بالجرائم الإلكترونية حديث النشأة، وإنّما قد يكون ضعفا وخوفا من الضحايا في الإبلاغ عما يتعرضون له من ابتزاز سابقا لعدم وجود قانون يحميهم، ومع وجوده أصبحوا يشعرون بالأمان والحماية ممّا شجعهم أن يبلغوا عن تعرضهم للابتزاز الإلكتروني، ومن هنا كان لا بد من ارتفاع نسبة الجرائم الإلكترونية في فلسطين.

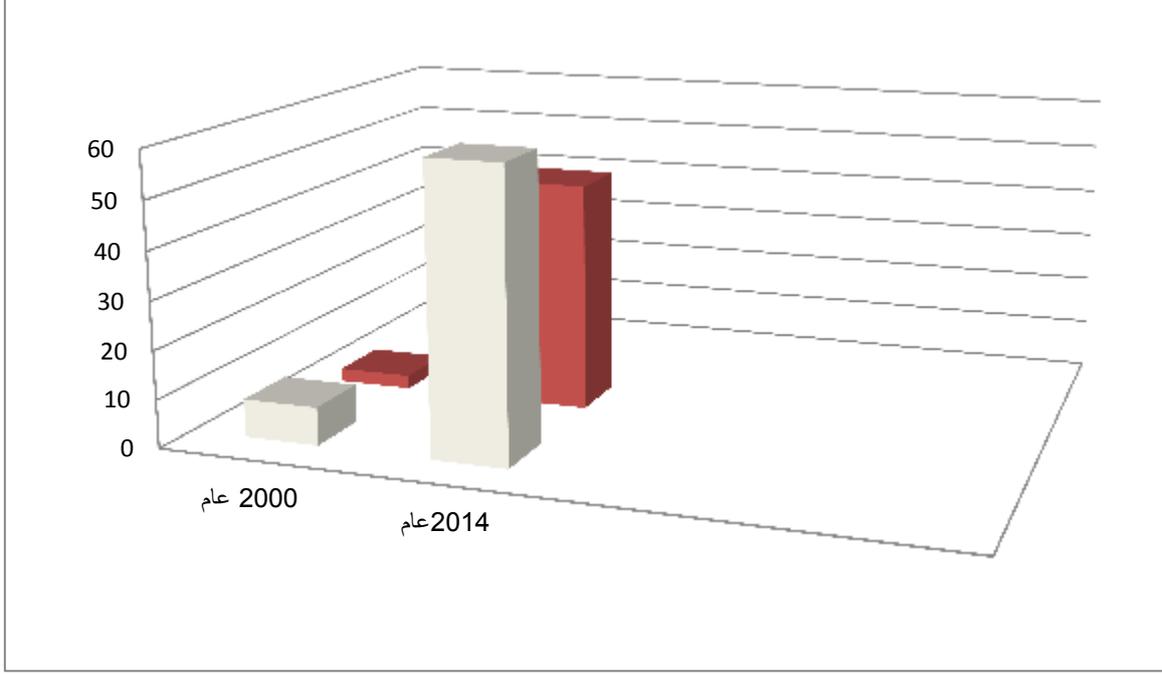
نلاحظ ممّا سبق الارتفاع المستمر للقضايا المسجلة على مرّ عدة سنوات لدى جهاز الشرطة الفلسطينية، ناهيك عن القضايا الخفية التي لا يتم تقديم شكاوي فيها خوفا من الفضيحة.

هذا الارتفاع يأتي نتيجة التطور الهائل في مجال التكنولوجيا وقطاع الاتصالات، وعدم وجود رقابة على الشبكة العنكبوتية، ممّا يتيح الفرصة أمام الجناة لتنفيذ هذه الجرائم بكل سهولة، لتنتج العديد من الأضرار والمساس بالخصوصية، في بداية الأمر كانت هذه القضايا تحدث بسبب غياب قانون رادع يحاسب مرتكبي هذه الجرائم وعدم وجود نصّ قانوني واضح حولها، ومن ثمّ تمّ نشر الوعي عن ضرورة الإبلاغ عن هذه الجرائم وعدم التعاطي مع الجاني، إضافة إلى تشكيل وحدة للجرائم

الإلكترونيّة لتكون مختصة في هذا المجال، وإصدار قانون رادع لهذا النوع من الجرائم بعقوبات مفصلة لكل فعل إجراميّ، ممّا زاد الوعي لدى أفراد المجتمع حول هذه الجرائم وطريقة التعامل معها وضرورة التبليغ عنها ممّا يفسر نسبة الزيادة بالقضايا المسجلة.

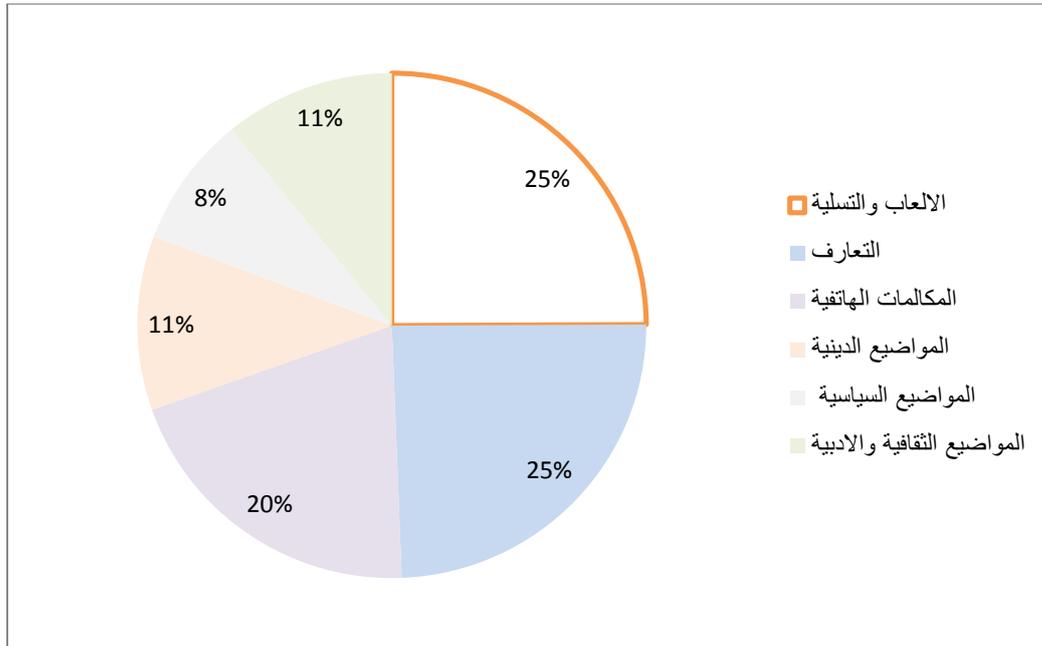
وحسب ما جاء في البيان الصحفي لـ (مركز الإحصاء الفلسطينيّ، 2014)، فإنّ تعريف الجريمة الإلكترونيّة يعني " أيّة مخالفة ترتكب ضدّ أفراد أو جماعات أو دول، بدافع جرمي ونية الإساءة الماديّة أو المعنويّة، سواء كان ذلك بطريقة مباشرة أو غير مباشرة، حيث يتم ذلك باستخدام وسائل الاتصالات المتنوعة والحديثة"، وبالاعتماد على إحصائيات الجهاز المركزي للإحصاء الفلسطينيّ وبناء على العديد من المتغيرات، نلاحظ بأنّه في عام (2014) كان عدد الحاسب الآلي لدى العائلات الفلسطينيّة (1.1) مليون حاسوب آلي بأنواعه المختلفة ما بين " كمبيوتر مكتبي، كمبيوتر محمول، وتابلت"، بينما بلغت نسبة العائلات التي تمتلك هاتفًا ذكيًا من إجمالي سكان دولة فلسطين المحتلة حوالي (51%) في ذات العام، بواقع (59.4%) في الضفة الغربية، و(34.7%) في قطاع غزة، مقارنة مع ما يقارب الثلث (32.8%) من العائلات في فلسطين كان لديها جهاز حاسوب في العام (2006) (الجهاز المركزي للإحصاء الفلسطينيّ، 2014).

نلاحظ ممّا سبق التفاوت في النسب ما بين الضفة الغربية وقطاع غزة ذلك بسبب اختلاف الوضع الاقتصاديّ والحصار المفروض على قطاع غزة ممّا جعل هناك عدم مقدرة على توفير أجهزة كمبيوتر بمختلف أنواعها على العديد من العائلات التي لا تمتلك سوى قوت يومها، حيث يظهر مقدار الزيادة في امتلاك حاسب آلي وهاتف ذكي من عام (2004) إلى عام (2014)، ممّا يعني زيادة مستخدمي الإنترنت وزيادة فرص تعرضهم للجرائم الإلكترونيّة من ضمنها جرائم الابتزاز الإلكترونيّ، حيث ارتفعت نسبة مستخدمي الإنترنت من كلا الجنسين في العام (2014) مقارنة في عام (2000)، بين الذكور من (7.9%) إلى (59.6%) بينما ارتفعت النسبة بين الإناث من (2.8%) إلى (47.5%)، أي النسبة الأعلى لاستخدام الإنترنت تعود إلى الذكور، لمزيد من التوضيح انظر/ي شكل رقم (1)، حيث كان يُعتبر في بداية الألفية أن استخدام الإناث للإنترنت أمر غير محبب وغير مباح، نتيجة القوالب المجتمعية وتقيدهم بالعادات والتقاليد الواهية التي ترفض كلّ ما هو جديد وتقيد الإناث وتصرفاتهنّ، ممّا جعل الإنترنت غير متاح للعديد منهنّ.



شكل رقم (1) يوضح نسبة مستخدمي الإنترنت من كلا الجنسين في فلسطين في عام 2014 مقارنة بعام 2000. بالاعتماد على الإحصائيات نلاحظ أنّ نسبة الأفراد الذين يستخدمون مواقع التواصل الاجتماعيّ (75.1) من مجمل مستخدمي الإنترنت في فلسطين، حيث إنّ (75%) يستخدمونها للتعارف، و(76.5%) يستخدمونها بغرض الألعاب والتسلية و(62%) بغرض الاتصال والمراسلات لعام (2014) (الجهاز المركزي للإحصاء الفلسطينيّ، 2014).

إنّ ما سبق يوضح أنّ النسبة الأعلى للغرض من استخدام مواقع التواصل الاجتماعيّ تعود للتعارف إذ تشكل (75%) من مجمل الاستخدام، أي أنّ الهدف الأساسي لهم هو التعارف، الذي يحمل في طياته بعض المخاطر خاصة لمن لا يملك مستوى عالياً من الذكاء العاطفيّ والثقة بالنفس والمستوى التعليميّ، فذلك يجعله أكثر عرضه لأنّ يكون ضحية سهلة لمستخدمي مواقع التواصل الاجتماعيّ الذين يحملون أهدافاً وغايات غير سوية نحو الآخرين.



الشكل رقم (2): الغرض من استخدام مواقع التواصل الاجتماعي

أما فيما يتعلق بجنس المجني عليه الذي قام بتقديم الشكوى نتيجة تعرضه لإحدى الجرائم الإلكترونية المختلفة حسب إحصائيات (جهاز الشرطة الفلسطينية، 2019)، حيث يوضح الجدول التالي أهم الشكاوي المقدمة حسب جنس الضحية ونوع الجريمة الإلكترونية:

جدول رقم (1.2): الشكاوي المقدمة حسب جنس الضحية ونوع الجريمة الإلكترونية:

الجنس	نوع الجريمة	ذكر	أنثى	غير ذلك	المجموع
إبتزاز إلكتروني		120	85	3	208
انتحال الشخصية		158	178	5	341
تشهير		236	136	28	400
تهديد		224	278	5	507

نلاحظ من الجدول رقم (1.2) أنّ نسبة الذكور المقدمين الشكوى أكثر من الإناث، قد يعود السبب في هذا التفاوت إلى خوف الإناث من الفضيحة والعار الذي قد يصل ببعض الأحيان إلى قتلها بسبب العادات والتقاليد ممّا قد يدفعها للتعاون مع الجاني وتحمل العذاب النفسي وتنفيذ مطالبه حتى لا تصل فضيحتها إلى أهلها ومجتمعها التي قد يترتب عليها طلاق أو تفكك أسري أو عقاب شديد، بالمقابل لا يتم معاملة الذكور بذات الطريقة عند تعرضهم للجرائم الإلكترونية ممّا يتيح الفرصة لهم بالتبليغ وتقديم الشكاوي دون تردد، بسبب القوالب النمطية الموجودة في المجتمعات العربية التي تتميز بالتسلط الذكوري تمتنع الأنثى عن التبليغ بتعرضها للابتزاز، إذ لا يمكن التهاون مع أي اثني تقع بهذا الفخ ففي أحيان كثيرة قد يتم هدر دمها تحديدا في القضايا التي تتعلق بالشرف دون الأخذ بعين الاعتبار إنها ضحية.

11.2.2 أنواع الجرائم الإلكترونية في فلسطين:

تنوعت وتعددت الجرائم الإلكترونية بسبب تطور التقنيات التكنولوجية المستمرة، ولعل من أهم تلك الأنواع في فلسطين ما يلي:

- **جرائم تقع على الحاسب الآلي:** "يقصد بها الأفعال التي تُشكل جريمة على أجهزة الحاسب الآلي، سواء على مكوناته مثل وسائل التخزين المرنة أو الصلبة أو الشاشة أو الطابعة"، أو على مكوناته المعنوية كالبيانات والمعلومات المخزنة داخل الحاسب الآلي".
- **جرائم تقع على الشبكة العنكبوتية (الإنترنت):** "هي كلّ فعل غير مشروع يقع على شبكة الإنترنت المختلفة والمتنوعة بقصد تعطيلها أو تخريبها أو تعديلها، بالإضافة لاستخدام عناوين وهمية إلكترونية غير حقيقية لدخول الشبكة، واختراق البريد الإلكتروني ومواقع التواصل الاجتماعي التي تمس بكرامة الأشخاص وتمس بخصوصيتهم وابتزازهم".
- **جرائم بواسطة شبكة الإنترنت:** "هي كلّ فعل غير مشروع يقع على وثيقة أو نص موجود بالشبكة العنكبوتية (الإنترنت) من أمثله "انتهاك الملكية الفكرية"، يتطلب ارتكابها اتصال بالإنترنت واستخدام الحاسب الآلي للوصول إلى قواعد البيانات للاطلاع عليها أو تغييرها".
- **الجرائم المتعلقة باستخدام الحاسب الآلي:** "هي الجرائم التي يستخدم فيها الحاسب الآلي كوسيلة لارتكاب الجريمة من أشكالها الاحتيال والتزوير"، إذا مصطلح جرائم الحاسب الآلي يستخدم للدلالة

على كلّ صور جرائم الحاسب الآلي سواء أكان الحاسب هدفا صريحا للفعل الإجرامي أم وسيلة له" (الأوجلي، 2006:5).

12.2.2 الصعوبات التي تواجه أصحاب الاختصاص في مكافحة جرائم الابتزاز الإلكتروني في فلسطين وطرق مكافحتها:

هناك العديد من الصعوبات التي تحدّ من عمل وحدتيّ: الجرائم الإلكترونية في النيابة العامة والشرطة الفلسطينية وحماية وحدة الأسرة في جهاز الشرطة الفلسطينية أثناء مكافحة الجرائم الإلكترونية، من أهمها تداخل أرقام الهاتف الدولي لفلسطين مع دولة الاحتلال، ذلك نتيجة سيطرة دولة الاحتلال "إسرائيل" بدرجة كبيرة على فضاء الاتصالات والإنترنت في فلسطين، وخضوع جميع الاتصالات الفلسطينية للرقابة الإسرائيلية، ممّا ساعد دولة الاحتلال الإسرائيليّ على تشكيل الوحدة رقم (8200) للتجسس الإلكترونيّ لها، بالتالي تُعدّ إسرائيل المرتكب الأول والأكبر للجرائم الإلكترونية على الساحة الفلسطينية. (النعامي، 2007)

لكن، وعلى الرغم من انتشار الجرائم الإلكترونية خاصة جريمة الابتزاز الإلكترونيّ بشكل واسع ومحاولة مكافحتها، إلا أنّ هناك مجموعة من الصعوبات تحدّ من ملاحقة مرتكبيها من قبل وحدة مكافحة الجرائم الإلكترونية، ونيابة الجرائم الإلكترونية ولعل من أهمها:

• **الصعوبات الفنية:** يُقصد بها الصعوبات التي تواجه الجهات المختصة منها: نقص المهارات الفنية والتقنيّة لدى بعض الأفراد في الجهات المختصة، وتطور التقنيّات بشكل مستمر، وعدم القدرة على مواكبتها في التقنيّات الفنية لمكافحتها، وأن يكون المبتز من دولة أخرى. (الشويعر، 2003: 173).

• **الصعوبات الاجتماعيّة:** وتتمثل في خوف الضحيّة من الفضائح ووصمة العار التي قد تلحق بها، وعدم تحقيق العدالة عند التبليغ عن جرائم الابتزاز الإلكترونيّ، نتيجة عدم وجود ثقة في الجهات المختصة (الهيبي، 2005: 218).

• سيطرة دولة الاحتلال على الفضاء الإلكترونيّ ممّا يعيق الجهات المختصة الفلسطينية في الوصول الكامل للجرائم الإلكترونية.

- صعوبة ملاحقة الجناة إذا كانوا في قطاع غزة نتيجة الانقسام الفلسطيني.
- استخدام بعض الجناة بطاقات الهاتف SIM التابعة لشركات إسرائيلية، إضافة إلى الاشتراك مع نقاط بيع إنترنت من شركات إسرائيلية (النعامي، 2007).

أما فيما يخص الطرق والتقنيات التي تستخدمها وحدة نيابة الجرائم الإلكترونية، فهي على النحو التالي:

- **تتبع عنوان (IP):** ويتمثل بالحزم البيانية التي يقوم بأرسالها الجاني بوجهها لضحيته، حيث يسهم عنوان الـ (IP) في الحصول على الجهاز الذي تم ارتكاب الجريمة عليها من ثم الوصول لموقع الجاني والحصول على كافة الأدلة الإلكترونية المتعلقة بالجريمة (حجازي، 2005: 63).
- **استخدام الأدلة الإلكترونية:** المحادثات والصور التي يقدمها الضحية كأدلة لإثبات جريمة الابتزاز الإلكتروني عند قيام الجاني بالتخلص من الأدلة الموجودة على جهازه المستخدم بالجريمة.
- **برامج التتبع:** وهي برامج متخصصة تستخدمها الجهات المختصة في مكافحة جرائم الابتزاز الإلكتروني تسهم في محاولات الاختراق التي قد يقوم بها المبتز (الجاني)، حيث تتميز بقدرتها على تزويد الجهات المختصة أو الضحية بمكان المبتز وتاريخ حدوثه وعنوان الـ (IP) الخاصة بالمبتز (الشدي، 2000: 100).
- **أدوات الضبط:** وهي أدوات تسهم في ضبط الجريمة ومعرفة كافة المعلومات حولها.
- **أدوات مساعدة:** يوجد العديد من الأدوات التي تساعد الوحدة في استرجاع المعلومات المتعلقة بالجريمة، مثل: برامج كسر كلمة المرور، وبرامج الضغط، وفك الضغط.
- **أدوات فحص ومراقبة الشبكات IP-TCP،** وتستخدم في فحص البروتوكول في الشبكة التي تعرضت للجريمة، حيث بالإمكان مراجعة أي عملية حدثت عليها (حجازي، 2005: 65).
- متابعة البلاغات واتخاذ الإجراءات اللازمة لضبط المبتز.
- دعم الضحية وحمايتها.
- نشر قصص نجاح للتأكيد على أهمية التدخل المهني والمختص في الحد من جرائم الابتزاز الإلكتروني.
- حملات توعية مجتمعية لاكتساب ثقة المواطنين.
- تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

• رقم موحد للتبليغ عن الجرائم الإلكترونية (الهويل، 2009: 9).

نلاحظ ممّا سبق العديد من التقنيّات والأساليب التي تستخدمها وحدة الجرائم الإلكترونيّة في مكافحة جريمة الابتزاز الإلكترونيّ، حيث وفّرت الوحدة رقم موحد للتبليغ عن الجرائم الإلكترونيّة ممّا أسهم في الكشف عن الكثير منها بسرية تامة ومحافظة على هوية الضحيّة، حيث روّجت عنه من خلال حملات توعويّة حول مدى خطورة الجرائم الإلكترونيّة، وبخاصة جرائم الابتزاز الإلكترونيّ وكيفية التعامل مع المبتز، لكن حين يتعلق الأمر في الأدلة الإلكترونيّة وتتبع البروتوكول قد يتطلب الأمر التنسيق مع الطرف الإسرائيليّ لامتلاكهم تقنيّات متطورة خاصة عندما يكون مقدم البلاغ من الأفراد القابعين داخل الجدار ويكون الجاني متواجد في الضفة، أو قيام بعض الجناة باستخدام بطاقات الهاتف SIM تابعة لشركات إسرائيلية، إضافة إلى الاشتراك مع نقاط بيع إنترنت من شركات إسرائيلية ممّا يشكل صعوبة بالغة في حلّ هذا النوع من القضايا.

13.2.2 الجهود المبذولة لمكافحة الجرائم الإلكترونيّة في العالم ودولة فلسطين المحتلة:

تحتاج كلّ الدول لجهود مشتركة ودولية للقضاء على الجريمة، خاصة مع التطور التكنولوجي والعولمة، لذلك كان هناك حاجة ماسه لوجود كيان دولي يأخذ على عاتقه القيام بهذه المهام، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة، حيث تمتاز الجرائم الإلكترونيّة من ضمنها جريمة الابتزاز الإلكترونيّ بأنّها عابرة للحدود والدول، ونظرا لسرعة حدوث هذه الجرائم، فإنّ العثور على أدلتها في الدول المختلفة يحتاج إلى وقت طويل من الإجراءات والتعقيدات الإدارية ممّا يسمح للجناة بالإفلات أو بتأخير العثور أو حذف الأدلة الإلكترونيّة، وهذا الأمر يدعو إلى أهمية ضرورة التعاون والاتصال المباشر بين جهات الاختصاص في الدول المختلفة لمعالجة هذه المشكلة، هذه المهام تناط بالإنترنت وبالتعاون الأمني بين الدول، إذ تمّ تأسيسه كمنظمة شرطية في العالم ليقوم بتقديم المساعدة في مكافحة الجرائم العابرة للحدود الوطنية، حيث يتمتع ببنية تحتية متطورة تمكن قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجراميّة المتجددة. وتركز نشاط الإنترنت في عدة مجالات منها (الفساد، والمخدرات، والإجرام المنظم، وغسيل الأموال المرتبط بالتكنولوجية، والمجرمون الفارون من العدالة، وتهديد السلامة العامة، والإرهاب والاتجار بالبشر)، وتقع الأمانة

العامة له في ليون بدولة فرنسا، بينما لكل بلد عضو في الإنترنت مكتب مركزي وطني يعمل فيه عدد من ضباط الشرطة الوطنية ذوي التأهيل العالي (حمودة، 2008).

ويوجد العديد من الجهود الدولية والإقليمية المبذولة في مجال مكافحة الجرائم الإلكترونية، ولكن حجر الأساس والبداية الحقيقية كانت من خلال توقيع اتفاقية مجلس أوروبا للجريمة الإلكترونية المنعقد في تاريخ (2001/11/23)، من ثم تم عقد مؤتمر الأمم المتحدة العاشر لمنع الجريمة والعدالة الجنائية لعام (2005)، يليه مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية لعام (2010) حيث أدرج الجرائم الإلكترونية ضمن جدول أعماله، إضافة إلى العديد من مؤتمرات قمة دول مجموعة G-8، وتكوّنت هذه المجموعة من الدول القوية صناعيا في العالم (الولايات المتحدة الأمريكية، وألمانيا، واليابان، وروسيا، وإيطاليا، والمملكة المتحدة، وفرنسا، وكندا) بالعديد من المؤتمرات والجهود لإرساء قواعد مكافحة الجرائم الإلكترونية وأسسها في العالم ذلك على النحو التالي:

- 1) تم إنشاء فريق فرعي للجرائم الإلكترونية فانق التقنية (1997).
- 2) اجتماع لسنّ عشرة مبادئ لمكافحة جرائم الحاسب الآلي في واشنطن عام (1997).
- 3) قمة مجموعة G-8 لعام (2004) لتعزيز القوانين المحليّة من ثم تأسيس وبناء القدرات العالميّة لمكافحة الاستخدامات الإرهابيّة والإجراميّة للإنترنت.
- 4) بيان مجموعة G-8 لعام (2005) للتأكيد على أنّ الجهات التي تنفذ القانون عليها أن تستجيب بسرعة لتهديدات ومخاطر الجرائم الإلكترونية.
- 5) اجتماع مجموعة G-8 لعام (2006) في موسكو لمناقشة الجرائم الإلكترونية وقضايا الفضاء الإلكترونيّ.
- 6) اجتماع قمة مجموعة G-8 لعام (2006) في سانت بطرسبرغ لمكافحة الإرهاب من ضمنها إساءة استخدام الفضاء الإلكترونيّ.
- 7) اجتماع وزراء العدل والداخلية لدول مجموعة G-8 لعام (2007) في ألمانيا لتجريم أشكال معينة من الجرائم الإلكترونية خاصة الإرهابية منها .

8) قمة G-8 في إيطاليا لعام (2009) لمناقشة جرائم الإنترنت والأمن السيبراني.

9) قمة دول G-8 في فرنسا لعام (2011) للتأكيد على أهمية الاقتصاد العالمي الرقمي، مكافحة إساءة استخدام الإنترنت، أمن الشبكات، وحماية البيانات الشخصية (مركز معلومات G-8 ، 2011).

أما فيما يتعلق بجهود السلطة الوطنية الفلسطينية في مكافحة الجرائم الإلكترونية فتمثل بالتوقيع على العديد من الاتفاقيات الدولية والإقليمية والثنائية لمواجهة الجرائم العابرة للحدود، التي من ضمنها " الجرائم الإلكترونية" التي تستخدم الشبكة العنكبونية (الإنترنت) ك مسرح لتنفيذ الجريمة، بالإضافة إلى تلك الجهود التي قامت بها للحصول على اعتراف المنظمة الشرطة العالمية (الإنتربول) كدولة عضو في عام (2017)، مما تطلب التوقيع على مجموعة أخرى من الاتفاقيات والمعاهدات التي توجب عليها الالتزام بها عبر موازنة تشريعاتها الداخلية مع هذه الاتفاقيات، ضمن التشريعات الداخلية التي قامت بمواءمتها قانون الجرائم الإلكترونية لعام (2017) (الشلالدة والرعي، 2015: 16) ، إضافة للعديد من الاتفاقيات التي من أهمها ما يلي:

أولاً: الاتفاقيات الثنائية والإقليمية: إن هذا النوع من الاتفاقيات يساعد دولة فلسطين المحتلة في التعاون الأمني في الجرائم العابرة للحدود، تتعلق هذه الاتفاقيات بالجرائم الإلكترونية بشكل خاص والجرائم العابرة للحدود بشكل عام، و أهم ما تمّ التوقيع عليه هو:

1) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام (2010): تهدف هذا الاتفاقية إلى تعزيز التعاون العربي في مكافحة الجرائم الإلكترونية للمحافظة على الأمن العربي ومصالحه، يتم تطبيق الاتفاقية في الحالات الآتية:

• عند ارتكاب الجريمة الإلكترونية في أكثر من دولة، أو تمّ ارتكاب الجريمة بدولة معينة، وكان له أثر بدول أخرى.

• قامت بها مجموعة إرهابية موجودة في دولة ما ليصل الضرر لأكثر من دولة.

• تمّ التخطيط للجريمة الإلكترونية في دولة وارتكابها في دولة أخرى (الأمانة العامة لجامعة الدول العربية، 2010).

(2) الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية لعام (2010)، يتم تطبيقها في الحالات الآتية:

- الأفعال الإجرامية المعرفة في هذه الاتفاقية.
- الجريمة التي تم تنفيذها بأكثر من دولة.
- الجريمة التي تم الإعداد والتخطيط لها في دولة ما وتم تنفيذها بدولة أخرى (الشلالدة والرعي، (2015).

ثانياً: الاتفاقيات الدولية، حين ننتبع تاريخ فلسطين في مجال الاتفاقيات الدولية نلاحظ قيامها بالتوقيع على مجموعة من الاتفاقيات والمعاهدات والمواثيق الدولية في مجالات مختلفة، حيث قامت فلسطين بالتوقيع على اتفاقية الأمم المتحدة بالتوقيع على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة غير الوطنية لعام (2000)، التي دخلت حيز النفاذ عام (2003)، وقد خلت موادها من نصوص صريحة فيما يتعلق بالجرائم الإلكترونية، تفرض هذه الاتفاقيات التزامات على دولة فلسطين بتعديل القوانين الفلسطينية بما يتماشى مع أحكام الاتفاقيات التي أصبحت فلسطين فيها طرفاً، حيث سعت الأمم المتحدة إلى الحفاظ على الأمن والاستقرار من خلال كثير من المؤتمرات والاتفاقيات في مجالات مختلفة، من أهم المؤتمرات مؤتمر هافانا لسنة (1990) في مكافحة جرائم الحاسب الآلي، من ثم المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين الذي عقد في القاهرة عام (1995).

شهدت نهاية عام (2014) وبداية عام (2015) توقيع فلسطين العديد من الاتفاقيات والمواثيق الدولية في مختلف المجالات، لكن كان الكثير من تلك الاتفاقيات يتوقف التوقيع عليها حصول فلسطين على الاعتراف بها كدولة في الجمعية العامة للأمم المتحدة، بعد التصويت على عضويتها في الجمعية العامة للأمم المتحدة اكتسبت فلسطين صفة الدولة مما أتاح لها الانضمام إلى هذه المعاهدات التي لا تتطلب سوى صفة الدولة سواء أكانت دولة عضو أم غير عضو في الجمعية العامة للأمم المتحدة.

إذ يتم تطبيق المعاهدات الدولية بعد إبرامها وجعلها قابلة للتنفيذ في إقليم الدولة في مختلف الميادين المطلوبة خصوصاً القضائية منها وفقاً لقوتها القانونية التي عادة ما يحددها دستور الدولة، فبعض الدول أكدت دساتيرها على أنّ قيمة المعاهدة الدولية (أي كان تسميتها اتفاقية أو معاهدة أو بروتوكول... الخ) أعلى من القوانين العادية وأقل من الدستور مثل فرنسا، وأخرى مثل مصر والعراق جعلت لهذه

الاتفاقيات قوة تعادل قوة القوانين العادية، بينما خلى القانون الأساسي المعدل لعام (2003) (دستور فلسطين المؤقت) من بيان قيمة الاتفاقيات والمعاهدات (البصيصي، 2015).

نتج عن هذه الحاجة ما يسمى بالمنظمة الدولية للشرطة الجنائية (الإنتربول)، ترجع بداياته لعام (1904) عندما تم إصدار الاتفاقية الدولية المتعلقة بمكافحة الرقيق البيض في (18/5/1904)، بعد ذلك قام الإنتربول بعقد مؤتمره الأول موناكو (14-18/4/1914) الذي ضم رجال الشرطة والقضاء والقانون من (14) دولة، لمناقشة أسس التعاون الدولي في المسائل الشرطية، وفي إمكانية مكتب دولي للتسجيل الجنائي وتنسيق إجراءات تسليم المجرمين، لكن لم يتم تسجيل أي نتيجة للمؤتمر بسبب قيام الحرب العالمية الأولى (الصاوي، 2000:648).

نلاحظ ممّا سبق أنّه رغم سنّ القوانين وانتشار الاتفاقيات إلا أنّ الجرائم الإلكترونية وتحديدًا جريمة الابتزاز الإلكترونيّ في تزايد مستمر، وذلك نتيجة التطور المستمر والمتسارع للتكنولوجيا وتقنياتها وانتشار التعليم حول هذه التقنيات، إذ أصبح بإمكان أي فرد حول العالم تعلم تصميم تقنيات وتطبيقات وبالتالي تعلم كيفية اختراقها والاستيلاء عليها، إضافة إلى انتشار استخدام الإنترنت، والهواتف الذكية لكافة الأعمار دون وجود رقابة أسرية على الاستخدام ومحتوى هذه الهواتف، ممّا يتيح الفرصة للجناة استدراج الضحايا واختيارهم بكل سهولة وتطبيق جريمتهم، لكن علينا الأخذ بعين الاعتبار ضعف تقنيات بعض الجهات المختصة في هذا المجال وعدم متابعة التطورات السريعة، وعدم وجود نصّ قانوني واضح يجرم هذه الأفعال أو وجوده لكن ضعف في تطبيقه.

3.2 مواقع التواصل الاجتماعي:

1.3.2 مقدمة:

نشأت الشبكة العنكبوتية (الإنترنت) في بدايتها لأهداف عسكرية، ومن ثم قدمت خدمات تعليمية لبعض الجامعات العالمية لتسمى مرحلة الويب (1)، وتطورت بعد ذلك وأصبح هناك حاجة لتقديم خدماتها لجميع فئات المجتمع حول العالم، وصولاً لمرحلة الويب (2) التي طرحت مواقع التواصل الاجتماعي نتيجة الحاجة الملحة لاستخدام الشبكة العنكبوتية (الإنترنت)، حيث أتاح التواصل والتفاعل بين مستخدميها، تتنوع أشكال وأهداف تلك المواقع الاجتماعية، فبعضها عام يهدف إلى التواصل العام

وتكوين الصداقات حول العالم، وبعضها الآخر يركز حول تكوين مواقع اجتماعية في نطاق محدود ومنحصر مثل مواقع المحترفين، والبعض الآخر يقدم خدمات متعددة مثل الإعلانات، والبيع والشراء، وتبادل المعلومات المختلفة، الأمر الذي جعل من هذه المواقع ضروريا للمجتمعات، ولا يمكن الاستغناء عنها (كاتب، 2011: 9).

ولعل الثورة الحقيقية للشبكة العنكبوتية (الإنترنت) كما يذكر (الخادمي، 2006: 21) بدأت عام (1993)، فقد تمّ اختراع وتأسيس الشبكة العنكبوتية التي بدأت بتقديم الخدمات للمستخدم وإتاحة الفرصة له لمشاهدة الصور، والرسومات، والصوت، والأفلام المتحركة، وقراءة النصوص".

لذلك نجد ممّا سبق أن الشبكة العنكبوتية (الإنترنت) عبارة عن "مجموعة من الشبكات العالمية المتصلة بملايين الأجهزة حول العالم، لتشكل مجموعة من الشبكات الضخمة، التي تنقل المعلومات دائمة التطور بسرعة فائقة بين دول العالم المختلفة".

ممّا سبق يتضح لنا أنّ الإنترنت عبارة عن شبكة اتصال عالمية تضم الملايين من أجهزة الحاسب الآلي المتصلة مع بعضها بعضا، وبواسطتها يستطيع الأفراد الدخول والتسجيل لمواقع التواصل الاجتماعي واستخدامها في مجال التواصل الاجتماعي والبيع والشراء والإعلانات، ونقل واستقبال المعلومات والملفات على اختلاف أنواعها، حيث أنّه ومع التطور التكنولوجي المستمر أصبح استخدامها يحمل في طياته شقين هما:

- الجيد والمفيد، ينتج في حال الاستخدام الصحيح لها، وفي حال استخدم الفرد الشبكة العنكبوتية (الإنترنت) لإرسال واستقبال المعلومات والملفات بطريقة صحيحة فهو يحمي نفسه من أن يكون ضحية لأي نوع من أنواع الجرائم الإلكترونية.
- السيء (غير المفيد)، الذي ينتج عن الاستخدام الخاطئ وغير الواعي لها، وهذه النقطة عكس النقطة السابقة، ونتيجة الاستخدام الخاطئ قد يقع الفرد ضحية للجرائم الإلكترونية، وهذا ما تمّ الحديث عنه في عنوان الاستخدامات الإيجابية والسلبية لمواقع التواصل الاجتماعي عبر الشبكة العنكبوتية.

2.3.2 مفهوم مواقع التواصل الاجتماعي:

يطلق على مواقع التواصل الاجتماعي بالإنجليزية "Social Network"، تم تأسيسها في البداية الأمر حتى يستطيع الفرد التعبير عن ذاته والتعارف والتواصل ما بين الأفراد ذوي الاهتمامات المشتركة، لكن مع تزايد أعداد المستخدمين والحاجات المتولدة بسبب التطور التقني والتكنولوجي نتج العديد من الاستخدامات المختلفة والمتنوعة: (التعليم، والعمل، والتعارف،..الخ).

أشار إليها (الدليمي، 2011:183) على أنها "مواقع تفاعلية لأنها تتيح الاتصال والتواصل لمستخدميها في أي وقت ومكان بالعالم، حيث ظهرت الشبكة العنكبوتية (الإنترنت) منذ سنوات وقد مكنتهم أيضا من التواصل المرئي والصوتي وتبادل الصور، وغيرها من الإمكانيات والخيارات التي توطد العلاقات الاجتماعية بينهم"، وهي نوع من أنواع التواصل بحسب (شقرة، 2014:60) " لأنها تقوم بالتواصل بعدة طرق (كتابة، وصور، وصوت) مع من يريد، بحيث يمكن تبادل الأفكار والآراء والمشاعر، واستخدامها للترويج عن النفس، أو للترويج عن المنتجات من خلال شبكة الإنترنت (العنكبوتية)"، بينما أشار إليها (أبو شعبان، 2013: 45) على أنها "خدمة إلكترونية لأنها تقوم بتقديم خدمات للمستخدمين من تواصل وتفاعل وإنشاء وتنظيم ملفات شخصية".

في حين يمكن تعريفها إجرائياً على إنها مواقع إلكترونية متصلة بالشبكة العنكبوتية، تمكن الفرد من إنشاء حساب شخصي فيها للتواصل والتعارف أو للعمل أو للدراسة، حيث تتميز هذه المواقع بسهولة استخدامها وانعدام تكلفتها.

3.3.2 أنواع مواقع التواصل الاجتماعي ومميزاتها:

تعتبر مواقع التواصل الاجتماعي من أكثر المواقع على شبكة الإنترنت انتشاراً واستمراراً، لأنها تتمتع بخاصية التواصل بين الأفراد والجماعات المستخدمين لها، حيث تمكنهم من التواصل وتبادل الأفكار والآراء والمعلومات والملفات والصور وأفلام الفيديو والتعبير عن الحالات والمشاعر الخاصة بهم، وهي متعددة ومتنوعة لعل من أهم أنواعها ما يلي:

- **موقع الفيس بوك:** يعدّ من أشهر المواقع الاجتماعية في العالم، تمّ إطلاقه في شهر فبراير من عام (2004)، يمكن من خلال هذا الموقع الاجتماعي أن يقوم المشترك بإضافة الأصدقاء إلى

ملفه الشخصي، ويقوم بتحديثه بشكل دوري، ويصل هذا التحديث إلى جميع أصدقائه وأصدقاء أصدقائه، بالإضافة إلى التواصل ومشاركة الصور والفيديو، ومشاركة الحالات بالإضافة إلى مشاركة موقعه على الخارطة (القرني، 2011:86).

• **موقع توتير:** هو أحد مواقع التواصل الاجتماعيّ تأسس في عام (2006)، أخذ توتير اسمه من مصطلح (تويت) الذي يعني (التغريد)، وهي خدمة مصغرة تسمح للمستخدمين إرسال رسائل نصية قصيرة لا تتعدى (140) حرفاً للرسالة الواحدة، يمكن لمن يمتلك حساب على توتير أن يتبادل التغريدات "التويتات" من خلال ظهورها على صفحاتهم الشخصية، أو في حالة عدم دخولهم على صفحة المستخدم صاحب الرسالة، وتتيح شبكة توتير خدمة التدوين المصغرة هذه، وإمكانية الردود والتحديث من خلال البريد الإلكترونيّ (المنصور، 2012:82).

• **موقع انستجرام:** هو عبارة عن تطبيق يسمح للمستخدم بأخذ الصور وإجراء التعديلات الرقمية والفلتر عليها حسب الرغبة، من ثم مشاركتها مع الأصدقاء عبر مواقع التواصل الاجتماعي، بدأ تطوير هذا التطبيق في العام (2010) بشكل خاص لأجهزة آبل (الأيفون، آيباد، آيبود)، بهدف تقديم طريقة مباشرة لمشاركة الصور الموجودة على الأجهزة مع قائمة الأجهزة الخاصة على مواقع التواصل الاجتماعيّ المختلفة، حين لقي هذا التطبيق رواجاً بدأ بتطوير نسخة أخرى منه للعمل على الأجهزة التي تدار بنظام تشغيل اندرويد (شقرة، 2014:79).

• **موقع اليوتيوب:** تأسس على يد ثلاثة موظفين كانوا يعملون في شركة باي بال عام (2015) في ولاية كاليفورنيا في الولايات المتحدة الأمريكية، يعتمد اليوتيوب في عرض المقاطع المتحركة التقنية (أدوب فلاش)، يشتمل الموقع على مقاطع متنوعة من الأفلام والموسيقى وفيديو لمستخدمي موقع اليوتيوب، أصبح من أهم مواقع التواصل الأولى حسب اختيار مجلة تايم الأمريكية (المنصور، 2012:87)

نلاحظ ممّا سبق العديد أن مواقع التواصل الاجتماعيّ (الفييس بوك، التوتير، انستجرام، اليوتيوب) هي الأكثر شهرة بسبب أقدميتها وتطورها بشكل مستمر، لكن أهم ما يميز مؤسسيها بأن لديهم القدرة على تطويرها بشكل دائم بما يتناسب مع احتياجات المستخدم وتلبية رغباتهم التي تتطور باستمرار، ممّا نتج عن ذلك الملايين من المستخدمين حول العالم، حيث أنّه يوجد العديد من مواقع التواصل

الاجتماعي الأخرى (الفايبر، وفليكر، وبلازك، وميكسي، وماي سبيس) لكن لم تحقق عدد مستخدمين مقارنه بمواقع التواصل الاجتماعي المذكورة أعلاه.

أما فيما يتعلق بـمميزاتها فتتميز مواقع التواصل الاجتماعي بالعديد من الخصائص والمميزات التي جعلتها تتمتع بالشعبية مقارنة بالمواقع الأخرى، لعل من أهم ما يميزها ما يلي:

• **العالمية:** أصبح بالإمكان الاتصال والتواصل مع أي فرد بأي مكان في العالم دون قيود أو حواجز جغرافية.

• **التفاعلية:** يتمتع مستخدم مواقع التواصل الاجتماعي بالقدرة على الاتصال والتفاعل مع فرد معين أو مجموعة وانتظار الرد.

• **مجانية الاشتراك:** تتمتع أغلبية مواقع التواصل الاجتماعي بمجانية الاشتراك.

• **سهولة الاستخدام:** بإمكان كافة الفئات العمرية استخدامها بسهولة.

• **التنوع وتعدد الاستعمالات:** يستخدمها كل فرد بناء على الهدف الذي يريده، فمنهم من يستخدمها للتواصل ومنهم من يستخدمها للتعليم ومنهم للعمل (الشاعر، 2015: 67).

نلاحظ بأن المميزات السابقة هي من جعلت مواقع التواصل الاجتماعي الأكثر شعبية في الاستخدام خاصة فيما يتعلق بمجانية استخدامها والاشتراك فيها (التسجيل فيها)، وسهولة استخدامها لكافة الأعمار دون إيجاد صعوبة في ذلك، إضافة إلى امتلاكها صفة التفاعلية بين العديد من الأطراف مما يجعلها مشجعة للاستخدام ومنتشرا بشكل كبير.

4.3.2 الاستخدامات الإيجابية والسلبية لمواقع التواصل الاجتماعي:

إن استخدام مواقع التواصل الاجتماعي يحمل في طياته الإيجابيات والسلبيات التي تتبع من هدف وطريقة استخدام الفرد لها، حيث بإمكانه استخدامها للاستفادة منها في التواصل مع أصدقائه وأقاربه خاصة من يقيمون في مناطق بعيدة أو للدراسة والعمل، وبالإمكان استخدامها بطرق سلبية ترجع بضرر على المستخدم لتجعله ضحية أو جاني ينتهز الفرصة المناسبة، لعل من أهم الإيجابيات التي يحصل عليها الفرد من استخدامه الصحيح لمواقع التواصل الاجتماعي ما يلي:

- **الأخبار المحليّة والدوليّة:** حيث أصبحت مواقع التواصل الاجتماعيّ تتمتع بالعديد من المنصات الإخبارية التي تنشر الأخبار بشكل مستمر ومجاني.
- **التعليم:** قامت العديد من الجهات التعليميّة كالجامعات والمعاهد والمدارس باستخدام مواقع التواصل الاجتماعيّ للتواصل مع طلابهم وإخبارهم بالمستجدات الدورية والطارئة، إضافة إلى تعزيز التفاعل بين الأفراد غير القادرين على التعليم والاستفادة من غيرهم وتنمية مهاراتهم.
- **الاستخدام الشخصي (الفردية):** يستطيع الفرد استخدام مواقع التواصل الاجتماعيّ بشكل شخصي (فردية) للتواصل المباشر وتبادل المعلومات والملفات والتواصل مع عائلته وأصدقائه وزملائه.
- **الجهات الحكومة:** قامت العديد من الجهات الحكوميّة باستخدام مواقع التواصل الاجتماعيّ للتواصل مع المراجعين والمجتمع كافة لإعلامهم بألية عملها وأماكن التواجد وأيام الدوام وأيام العطل (الظهواني، 2016).

يمكن القول إنّ هناك العديد من الإيجابيات التي قد يحصل عليها الفرد عند استخدام مواقع التواصل الاجتماعيّ، حيث قامت العديد من الجهات والمؤسسات في الدولة باستثمار مواقع التواصل الاجتماعيّ للإعلان والترويج عن نفسها خاصة (المؤسسات الحقوقيّة، والتعليميّة، والإعلاميّة، والمؤسسات المحليّة والحكوميّة)، إضافة إلى تواجد صفحات متخصصة في العديد من المجالات، لذا نجد مواقع التواصل الاجتماعيّ متداخلة في العديد من مناحي الحياة، حيث أتاح الفرصة أمام الجميع إلى (التواصل، والتعلم، والإبداع، والشعور بالانتماء، والشعور بالهوية المجتمعيّة) من خلال التفاعل وتعزيز العلاقات الاجتماعيّة.

أما فيما يخص أهم السلبيات لاستخدام مواقع التواصل الاجتماعيّ فهي كالآتي:

- **زيادة الجرائم الإلكترونيّة:** حيث أتاحت مواقع التواصل الاجتماعيّ والتطورات التقنيّة والتكنولوجيّة العديد من الفرص لارتكاب الجرائم لضعاف النفوس ممّا زاد نسبة ارتكاب الجرائم بشكل عام والجرائم الإلكترونيّة بشكل خاص، ومع التطورات والتقنيات الحاصلة تنوعت الجرائم الإلكترونيّة واختلفت أداؤها وغايتها فمنها: جرائم ماليّة، وسياسيّة، وجنائيّة، وجرائم الابتزاز الإلكترونيّ، والنصب والاحتيال، والتحرش الإلكترونيّ (السويدي، 2013: 18).
- **الانعزال والاعتراب النفسيّ والاجتماعيّ:** قام العديد من الأفراد خاصة الشباب منهم باستخدام مواقع التواصل الاجتماعيّ بشكل كبير حتى وصل بهم الأمر إلى مرحلة الإدمان، ممّا أثرت بشكل سلبي

على حياتهم وعلاقاتهم الاجتماعية والأسرية، خاصة الذين يطلعون على الثقافات المختلفة ويتأثرون بها بشكل سلبي وغير واعي، مما يؤدي إلى ظهور بعض مظاهر الاغتراب النفسي والاجتماعي لديهم، فتكون البداية بالانعزال عن أسرته وأصدقائهم من ثم الاغتراب عن مجتمعهم لرغبتهم بالتواجد في مجتمعات أخرى بظروف يتمنونها (الساري، 2009: 3).

- **الإدمان الإلكتروني:** قد يقوم بعض الأفراد في تكريس يومه لاستخدام مواقع التواصل الاجتماعي دون الإحساس بالوقت الذي يقضيه أثناء استخدامه فيصل به الأمر إلى مرحلة الإدمان، فمن الممكن أن تصيبه أعراض الإدمان كالصداع والتوتر والعصبية، نتيجة الاستخدام الخاطئ وغير الواعي (السويدي، 2013: 17).
- **الإباحية:** تتميز مواقع التواصل الاجتماعي بضعف الرقابة على محتواه مما أدى إلى انتشار آفة الإباحية بشكل كبير سواء من خلال المواقع والصفحات المتخصصة في بيع الهوا أو نشر مقاطع إباحية، أو قد يكون ذلك من خلال العلاقات غير الشرعية التي تنتج من خلال التواصل الخاطئ بين الأفراد (الشميمري، 2010: 252).

5.3.2 النظريات المفسرة لجرائم الابتزاز الإلكتروني:

تتنوع وتتعدد النظريات المفسرة لجرائم الابتزاز الإلكتروني لعل من أهمها ما يلي:

- **نظرية الفرصة أو الأنشطة الروتينية (النشاط الرتيب):** أشهر روادها ماركوس فيلسون ولاريكوهين سنة (1979)، من أبعاد هذه النظرية أن النزعة أو الميل الإجرامي موجود لدى بعض الأفراد، لكنه بحاجة إلى ثلاثة عناصر أساسية لحدوثه، وهي:
 - الإرادة الإجرامية تتمثل في (الجاني).
 - الفرصة تتمثل في (وجود ضحية مناسب).
 - غياب الحراسة بمعنى (غياب القوانين الرادعة) التي من الممكن أن تقلل من ممارسة الأفراد للجريمة في المجتمع (Felson, and Cohen 1979: 589).

نلاحظ مما سبق أن الجريمة جزء لا يتجزأ من الحياة اليومية للأفراد، ولا يمكن أن تستمر الحياة دون التفاعل بين الأفراد، وبسبب تغيير في أنماط التفاعل الاجتماعي والتغيرات الاقتصادية والتقنية خاصة

والتطور التقني والتكنولوجي وانبثاق أنماط جديدة من النشاط الروتيني (اليومي) لحياة الفرد كاستخدام الوسائل التقنية الحديثة التي من ضمنها مواقع التواصل الاجتماعي التي انتشرت في المجتمع الفلسطيني بشكل خاص والعالم بشكل عام، ولكن هذا الاستخدام قد يحمل في طياته بعض المخاطر نتيجة الاستخدام الخاطئ والمستهتر، مما يتيح للجاني (المبتز) فرصة لمعرفة الأنشطة الروتينية المتكررة للضحية بكل بساطة من خلال التواصل مع الضحية أو مراقبة ما يتم نشره من خلال مواقع التواصل الاجتماعي أو حتى مراقبة الضحية خلال حياتها اليومية، كل ما سبق يصبح عبارة عن معلومات معلومة للمبتز عن الضحية مما يُشكل له فرصة لإبتزاز الضحية، فالمبتز يستغل الطرف الثاني (الضحية المناسبة) التي يراها فرصة متاحة له لضعفها وعدم قدرتها الدفاع عن نفسها، ويستغل غياب الرقابة على الشبكة العنكبوتية (الإنترنت) لإيقاعها بعلاقات غير شرعية تنتهي غالبا بالابتزاز والتهديد بالفضيحة إذا لم تحقق الضحية أهداف الجاني.

• **النظرية اللامعيارية أو الأنومي:** من أشهر روادها "أميل دوركايم وميرتون"، توضح هذه النظرية أنه نتيجة اختلال التركيب الاجتماعي الناجمة عن التطور الحضاري والتكنولوجي، تضعف وتختفي القيم والأعراف والتقاليد والمعتقدات، التي كانت رادعا للسلوك المنحرف في المجتمع، نتيجة لذلك لا يمكن قياس سلوك ما باعتباره سلوكا سويا أو غير سوي، مما يعني زوال الوسائل المتبعة في الضبط الاجتماعي، وقد يلاقي الأسوياء نتيجة ذلك صعوبة في تلبية احتياجاتهم، فيحدث قلق وتوتر لدى الفرد، بالتالي ارتبائه أو عزله عن المجتمع، وقد يصبح معاديا وغير مبالٍ، فتمزق وسائل الضبط الاجتماعي ينعكس على القيم التي تسنّها المجتمعات ليشبع الأفراد شهواتهم بطرق مشروعة، فينتج عن ذلك محاولة الأفراد تحقيق أكبر قدر ممكن من رغباتهم والوصول إلى أهدافهم دون وجه حق مما لا يستطيعون تحقيقه بالطرق المشروعة التي تحددها قيم المجتمع، بالتالي قد يلجأ البعض إلى ممارسة العديد من الجرائم لتحقيق رغباتهم بطرق غير مشروعة أو استخدام الشبكة العنكبوتية للهروب من واقعهم الذي لا يمكن تغييره (Kornhauser,1978).

مما سبق يتضح لنا أنّ الثقافة السائدة في المجتمع قد تتغير مع التغيير التكنولوجي والتقني الحاصل في مجتمعات العالم أجمع، من ضمنها المجتمع الفلسطيني الذي عاصر هذه التغيرات الهائلة، ونتيجة لتنوع الثقافات داخل المجتمع الفلسطيني إذ تختلف من قرية، لمخيم، لمدينة، أدى ذلك إلى انحلال القيم والمبادئ وبالتالي انحلال الروابط الاجتماعية التي كانت تسهم في ضبط الخلل وردعه، مما

أضعف الضبط الأسري، وكون غالبية الأسر الفلسطينية تتبع نمط الأسرة النووية، فقد نتج عدم حصول الأبناء على الدعم والمتابعة الكافية، وبسبب ظهور أنشطة روتينية يومية جديدة نتيجة للتغيرات التكنولوجية والاجتماعية، وتتفق هذه النظرية مع نظرية النشاط الرتيب فأصبحت بعض الأسر تتقبل أن يقوم فرد من العائلة بالارتباط عاطفياً مع الجنس الآخر وأرسال صورته إليه دون رقابة، ببعض الأحيان قد تكون خادشه للحياء مما يجعلهم مشاركين في وقوع الجريمة عليهم ومساهمتهم في حدوث الفعل الإجرامي كجرائم الابتزاز الإلكتروني، حيث كان تفاعلهم وإهمالها في حماية نفسها أحد أهم العوامل والأسباب التي أوقعتهم ضحايا لجرائم الابتزاز الإلكتروني.

• **نظرية التعلق:** من أهم روادها جون بولبي (1969)، تركزت هذه النظرية على أنّ الإنسان بحاجة إلى إن يبنى علاقات إنسانية ودية وثيقة وبخاصة العاطفية منها، يزداد هذا الشعور عند الإحساس بالخطر والتهديد أو في المواقف الضاغطة، مما يرفع مستوى التوتر لديه ويكون بحاجة إلى سد حاجته العاطفية من خلال التعلق بفرد معين دون الأخذ بعين الاعتبار المخاطر والخسائر التي قد تلحق به من هذه العلاقة (Leonhardt, Matthews, Meaney, & Walker, 2007).

نلاحظ مما سبق أن بعض الأفراد حين يشعرون بالخطر والتهديد أو يتعرضون للمواقف الضاغطة قد يلجئون إلى علاقات مع أفراد يتم اختيارهم بطريقة عشوائية، ذلك محاولة منهم للشعور بالأمان وخفض مستوى التوتر لديهم من خلال التعلق بفرد ما، لكن قد يتم الاختيار من خلال الاستخدام المتهور لمواقع التواصل الاجتماعي والتعرف على غرباء دون التفكير بالعواقب للحصول على علاقات يطمح من خلالها التخلص من التوتر والحصول على الأمان، وبهذا يكون على استعداد للقيام بما يمليه عليه الطرف الآخر دون الأخذ بعين الاعتبار أنّ هذه العلاقة قد تصل للاستغلال، نتيجة تدني مستوى الذكاء العاطفي لديه وعدم قدرته على حلّ مشاكله وإيجاد الحلول المناسبة، وعدم قدرته على التخلص من الخوف والتوتر لديه بنفسه وترجمة وفهم مشاعره ومشاعر الطرف الآخر، مما يجعله ضحية مناسبة لارتكاب جريمة الابتزاز الإلكتروني وحصول الجاني على مبتغاه دون تعب أو مجهود.

• **نظرية الاختلاط التفاضلي (1939) ونظرية التعلم الاجتماعي:** الاختلاط أو المخالطة التفاضلية من أبرز روادها "سدرلاند" حيث حاول صياغة نظرية تكاملية في السلوك الإجرامي وتفسيره، على أساس أنّ الفرد يصبح جانحاً بسبب اقتناعه بأفكار وتحديات مخالفة للقانون في إطار انعدام الرقابة المجتمعية والأسرية والذاتية نتيجة للتطورات الهائلة في المجال التقني والتكنولوجي والاستخدام الخاطئ

لها، أي أنه في حالة انعدام القيم والأخلاق نتيجة للتغيرات الحاصلة التي ينتج عنها عدم تنظيم اجتماعي وفقدان الرادع تنهياً الظروف والمواقف لانتقال بعض الأنماط السلوكية غير الصحيحة من أفراد غير أسوياء إلى أفراد أسوياء (هذا ينسجم ويتوافق مع منطلقات ومبادئ النظرية اللامعيارية التي ترى أنّ ممارسة الجريمة تتمّ عندما تضعف القيم والأخلاق في المجتمع)، هنا يرى "سذرلاند" أن فكرة عدم التنظيم الاجتماعي أي ضعف "الرقابة المجتمعية" ليست إلا حالة تفاضلية أو نسبية تتوقف على نوعية وماهية التركيب الاجتماعي الخاص بكل جماعة ذلك بالنسبة لمواقفها نحو القانون ومدى احترامها للنظام وكرهها لمن يخالفه. (Clark, 1972)، ممّا سبق ووفق هذه النظرية فإنّ استخدام مواقع التواصل الاجتماعي هي سلوك مكتسب يتعلمه الفرد من خلال اختلاطه بالآخرين ذلك من خلال عملية الاتصال والتواصل والتفاعل الاجتماعي بين الأفراد الذين ينتمون إلى الجماعة الواحدة أو المجتمع الواحد، وتتطلب عملية التعلم تلك علاقات متينة من الصداقة أو القرابة بين الأفراد، هذا يعني أن الفرد الذي يستخدم مواقع التواصل الاجتماعي يتمتع بعلاقات أولية مباشرة مع بعض الأفراد المنحليين الذين اكتسب منهم سلوك الاستخدام المتهور وغير الواعي لهذه المواقع، ويؤكد "سذرلاند" أنّ هذا النوع من السلوك يختلف ويتباين وفقاً لبعض العوامل التي تحيط بالفرد، فتكرار السلوك ومدته، وعمق الاختلاط وقوته أو قوة التأثير على الأفراد، هي عوامل مهمة تؤثر على اكتساب الفرد لهذا السلوك واستخدامه بطريقة خاطئة.

• **نظرية الاختيار العقلاني (1985):** من رواد هذه النظرية الباحثان "رون كلارك وكورنيس"، حيث كانت بدايتها من خلال رون كلارك الذي كان مقتنعا بقناعة تامة بأفكار نيومان التي تتمحور حول الوقاية الموقفية، لكن حين بدأ كلارك بالبحث والتوسع في هذا المجال أوجد التصور الأولي عن نظرية الاختيار العقلاني، من ثم بدء التأثير بالنظريات الأخرى مثل نظرية فيسلون التي أسهمت في تطوير نظريته وكملتها، حيث تركز هذه النظرية على مبدأ المنفعة التي يحصل عليه الفرد بأقل مجهود وتكاليف استناداً على حسابات عقلية دقيقة لمقدار المتعة والمنفعة لارتكاب الفعل الإجرامي، حين تتوفر الفرصة لذلك (طالب، 2001: 61-64).

ممّا سبق يتضح لنا أنّ هناك عدة عناصر هامة لارتكاب أي جريمة، ومن ضمنها الجريمة المستحدثة جريمة الابتزاز الإلكتروني، إلا وهي الفرصة لارتكاب جرائم الابتزاز الإلكتروني نتيجة غياب الحراسة والرقابة على مواقع التواصل الاجتماعي على شبكة الإنترنت، وقيام الجاني في حساب المنفعة والمتعة الحاصلة له من هذا الفعل، حيث تشكل العوامل السابقة الأساس للجاني لارتكاب

جريمته وتشكل ذات العناصر الهامة لارتكاب الجريمة في نظرية (الفرصة) ونظرية (الأنشطة الروتينية)، حيث يتمتع الجاني بالذكاء العاطفي الكافي الذي يدفعه إلى استغلال اللامبالاة التي يتمتع بها الضحية في عرض حياته والتواصل مع أفراد لا يعرفهم ويشاركهم حياته بتفاصيلها، ليقوم بفعلته مع حرصه الحصول على مردود أو غاية قد يكون جنسي أو مادي أو انتقام حسب غايته الأساسية من ارتكاب جريمة الابتزاز الإلكتروني.

• **نظرية تهور المجني عليه:** أول من أشار إلى دور الضحية واستفزازه وتهوره هو العالم "مارفن وولفغانق"، إنَّ أحد التفسيرات الرئيسية حول دور الضحية في حصول الفعل الإجرامي هو قيامه بالدور الاستفزازي من خلال أنه يبدأ بالمواجهة الاستفزازية سواء بالألفاظ أو بالحركات ثم يستجيب له الطرف الآخر في إيذائه وتهديده أو ابتزازه أو بقتله. (الشمري، 2011: 56)

يمكننا أن نستدل ممَّا سبق بأنَّ التهور في أسلوب الحياة أو قيام الضحية باستفزاز الجاني عامل مهم وله دور رئيسي في وقوع الفعل الإجرامي، أي أنه لولا الضحية لما وقعت الجريمة، حيث إنَّ الضحية تلعب دورا فعالا في حدوث جريمة الابتزاز الإلكتروني من خلال إثارها للجاني بأسلوب حياتها المتهور دون قيود وحدود لجعلها فريسة المنال له، أو قيامها بإرسال كلام أو صور أو إحياءات لاستفزازه خاصة في بعض العلاقات العاطفية التي قد تربط الضحية بالجاني، فعند محاولة الضحية الانفصال عنه أو عدم الانصياع لأهدافه وطلباته، قد ينتهي الأمر بابتزاز المجرم لها، واستغلالها لتحقيق أهدافه ورغباته رغما عنها خوفا من التهديدات والفضائح.

4.2 الدراسات السابقة وذات العلاقة:

1.4.2 الدراسات العربية:

دراسة النصر (2017)، بعنوان " التحقيق في جريمتي التحرش والابتزاز عبر الشبكات الإلكترونية - دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية".

هدفت الدراسة إلى التحقيق في جريمتي التحرش والابتزاز الإلكتروني عبر الشبكات الإلكترونية من خلال استجابات هيئة التحقيق والادعاء العام، استخدم الباحث المنهج الوصفي الارتباطي، وأداة الاستبانة لجمع المعلومات تكوّنت من (63) فقرة موزعة على أربعة محاور، حيث كان عينة الدراسة من محققي هيئة الادعاء العام البالغ عددهم (100) محقق، من أهم النتائج: أنّ مدى انتشار جريمة الابتزاز عبر الشبكات الإلكترونية من وجهة نظر المحقق في هيئة التحقيق والادعاء العام بالمنطقة الشرقية كان مرتفعاً، بينما التحرش الإلكتروني في ذات المنطقة متوسط، بالإضافة إلى ارتفاع مهارات التحقيق الجنائي في مواجهة جرائم الابتزاز والتحرش الإلكتروني من وجهة نظر المحققين، كذلك ارتفاع مستوى المعوقات التي تواجه المحققين أثناء التحقيق في جريمتي الابتزاز والتحرش الإلكتروني.

دراسة بنت حجاب (2016)، بعنوان " تصور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الابتزاز".

هدفت الدراسة بالخروج بتصور مقترح لتنمية الوعي الوقائي لدى الفتيات من جرائم الابتزاز، ومعرفة وعي فتيات الجامعة بأنواع جرائم الابتزاز وأشكالها، ومعرفة مدى الوعي الوقائي لديهن، تكوّن مجتمع الدراسة من طالبات كلية إدارة الأعمال بجامعة تبوك الواقعة المملكة العربية السعودية، حيث تمّ اختيار عينة الدراسة من خلال العينة العشوائية البسيطة وتكوّنت من (320) طالبة، واستخدمت الباحثة المنهج الوصفي المسحيّ بالإضافة إلى تصميمها أداة خاصة وهي استمارة قياس الوعي لدى الفتيات، من أهم نتائج الدراسة: وجود ضعف لدى الفتيات في جانب معرفة أنواع وأشكال جرائم الابتزاز الإلكتروني كافة، يوجد حاجة لتنمية الوعي الوقائي بجرائم ابتزاز الفتيات.

دراسة المطيري(2015)، بعنوان " المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي - دراسة مقارنة".

هدفت الدراسة إلى التعرف على ماهية المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي مقارنة بالقانون المصري، استخدم الباحث المنهج الوصفي التحليلي ذلك من خلال الرجوع إلى النصوص القانونية والنظامية في السعودية، توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها: وجود فجوة تشريعية بين دول العالم فيما يتعلق بمكافحة جرائم الإلكتروني مما أدى إلى زيادة هذه الجرائم، وصعوبة تتبع أثر الجاني إذا كان خارج الحدود الجغرافية بسبب اختلاف الجوانب الإجرامية في العالم واختلاف دوافع وأساليب الجاني، بالإضافة إلى ضعف في التعامل مع الأدلة من قبل بعض العاملين في الجهات الأمنية مما يؤدي إلى ضياعها أو فقدانها، ومقارنة القانون السعودي بالقانون المصري فيما يتعلق بجريمة الابتزاز الإلكتروني حيث وجد أنّ القانون المصري يعالج هذه الجريمة من خلال النصوص القانونية القديمة للجرائم التقليدية مما خلق قصور في معالجته.

دراسة المحمود(2014)، بعنوان " المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة - دراسة تأصيلية تطبيقية".

هدفت الدراسة إلى التعرف على وسائل التواصل الاجتماعي الحديثة، وبيان المسؤولية الجنائية لمستخدمي وسائل التواصل الاجتماعي، ومعرفة أبرز الجرائم الجنائية عند إساءة استخدام وسائل التواصل الاجتماعي وبيان عقوبتها، واستخدم الباحث المنهج الوصفي التحليلي الاستقرائي ومنهج تحليل المضمون في الجانب التطبيقي من الدراسة، ومن أهم نتائج الدراسة: بيان إيجابيات وسلبيات استخدام وسائل التواصل الاجتماعي، وتوضيح ما هي الجرائم التي قد يرتكبها مستخدم الوسائل التواصل الاجتماعي وعقوباتها وكيف تؤثر وسائل التواصل الاجتماعي في نشر الجرائم واستخدامها كوسيلة من وسائل الابتزاز الإلكتروني والتشهير والتهديد والتهديد إذا لم يستجيب الضحية للجاني، من أهم التوصيات: تدريب وتنقيف العاملين في المجال الجنائي على التعامل مع جرائم وسائل التواصل الاجتماعي، ومراجعة المواد الخاصة بتجريم وعقوبة الجرائم المعلوماتية.

دراسة الخليوي (2014)، بعنوان " دور مواقع التواصل الاجتماعي في زيادة جريمة الابتزاز ضد المرأة من وجهة نظر طالبات الجامعات السعودية ".

من أهداف الدراسة: التعرف على الآثار السلبية لمواقع التواصل الاجتماعي، وأهم العوامل التي تدفع الجاني لارتكاب جريمة الابتزاز ضد النساء، وأساليب الوقاية والمكافحة، واستخدام الباحث المنهج الوصفي، وتكوّن مجتمع الدراسة من جميع طالبات درجة البكالوريوس لجامعة الأميرة نورة، ومن النتائج التي توصلت لها هذه الدراسة ما يلي: أن مواقع التواصل الاجتماعي سهلت للمبتز تهديد الضحية، سهولة التواصل والتعارف وإقامة علاقات محرمة بين المبتز والفتاة، ضعف الوازع الديني لدى المبتز، وضعف العقوبات الرادعة لجرائم الابتزاز الإلكتروني، وضعف الرقابة الأسرية على الأبناء، العادات والتقاليد قد تخضع الفتاة للاستمرار في الخضوع للمبتز، التطور التقني ساعد في سهولة اتصال الشاب بالفتاة، لذلك على الأسرة تقوية الوازع الديني لدى أبنائها، واحتواء مشاكل الفتاة وتوعيتها بعواقب العلاقات العاطفية، وعلى الأسرة تفعيل دور الحوار.

دارسة الحقباني (2013)، بعنوان "مهارات البحث والتحقيق في الجرائم المعلوماتية- دراسة ميدانية أجريت على ضباط الشرطة بمدينة الرياض".

أهداف الدراسة: التعرف على خصائص الجرائم المعلوماتية ومن ضمنها جرائم الابتزاز الإلكتروني، والتعرف على درجة توافر مهارات البحث والتحقيق في الجرائم المعلوماتية لدى ضباط شرطة مدينة دبي والمعوقات. منهج الدراسة وأدواتها: استخدم الباحث المنهج الوصفي عن طريق مدخل المسح الاجتماعي باستخدام أداة الاستبانة، كما استخدم الباحث أسلوب تحليل المحتوى لدراسة وتحليل عدد من القضايا في الجرائم المعلوماتية، وتكوّن مجتمع الدراسة من الضباط العاملين بشرطة مدينة الرياض والبالغ عددهم (150) ضابطاً، وتم تطبيق هذه الدراسة على عيّنة مقدارها (140) ضابطاً، ومن أهم نتائج هذه الدراسة: يوافق أفراد مجتمع الدراسة (الضباط) على توافر المهارات العامة اللازمة للبحث والتحقيق في الجرائم المعلوماتية لديهم بدرجة متوسطة، ووجود معوقات تحدّ من تطوير هذه المهارات في البحث والتحقيق، الموافقة على السبل التي اقترحها الباحث لتطوير مهارات البحث والتحقيق.

دراسة العميرة (2012)، بعنوان " تجريم جرائم ابتزاز النساء - دراسة تأصيلية تطبيقية " .

من أهداف الدراسة: التعرف على مفهوم الابتزاز الإلكتروني النساء وأسبابه ووسائله وصوره ووسائل الوقاية، ومعرفة آثار جريمة ابتزاز النساء والجرائم ذات العلاقة، استخدم الباحث في هذه الدراسة المنهج الوصفي الاستقرائي لجمع المعلومات المتعلقة بموضوع الدراسة، والمنهج التأصيلي للتوضيح موقف الشرع والدّين، ومنهج تحليل المضمون لإكمال الجانب التطبيقي للبحث، وتكوّن مجتمع الدراسة من عشر قضايا تمّ الحكم فيها من خلال المحاكم الشرعية بالمملكة العربي السعودية، من أهم نتائج هذه الدراسة ما يلي: أغلب جرائم الابتزاز الإلكتروني تحدث بسبب وجود علاقة عاطفية بين الرجل والمرأة خارج إطار الزوجية، وتحمل المرأة المسؤولية الأكبر في أغلب جرائم الابتزاز الإلكتروني حيث إنّها السبب للوصول إلى صورها ومستندات السرية إلى يد المبتز، حيث تقدمه ببعض الأحيان للمبتز بسبب ارتفاع مستوى الثقة أو إساءة الاستخدام التقنية أو الإهمال.

دراسة الشمراني،(2011)، بعنوان " ظاهرة الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي".

هدفت الدراسة إلى التعرف على حجم ظاهرة الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي، من خلال التعرف إلى أسباب ظاهرة الابتزاز أساليب وأشكال الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي، أجريت الدراسة على عدد من الضباط العاملين في شرطة منطقة الرياض، واستخدام الباحث المنهج الوصفي التحليلي باستخدام الاستبانة كأداة لجمع البيانات، توصلت الدراسة إلى مجموعة من النتائج لعل من أهمها التهديد بنشر صور ومحادثات ورسائل عن طريق الهاتف المحمول، واستدراج النساء لمكاتب التوظيف الوهمية، والطرق المهمة لمواجهة الابتزاز في المجتمع السعودي هي تحسين مستويات الراتب المنخفض، تحديث الإجراءات القانونية لمحاسبة مرتكبي جريمة الابتزاز الإلكتروني.

دراسة الشمري(2011) بعنوان " دور الضحية في حصول الفعل الإجرامي من منظور طلاب الجامعة".

هدفت هذه الدراسة إلى التعرف على دور الضحية في حصول الفعل الإجرامي من منظور طلاب جامعة نايف العربية للعلوم الأمنية، وتكوّن مجتمع وعينة الدراسة من جميع طلاب الجامعة للعام الأكاديمي(2010-2011)، المسجلين في مرحلة الدبلوم والماجستير والدكتوراة لمختلف التخصصات

وكليات الجامعة لكلا الجنسين، أما عينة الدراسة، فتكوّنت من (481) طالباً، واستخدم الباحث المنهج الوصفيّ بأسلوب المسح الاجتماعيّ، واعتمد الباحث على الاستبانة كأداة للدراسة وجمع المعلومات الميدانيّة، ومن أهم نتائج الدّراسة: أنّ وجهة نظر الطلبة في حول دور الضحية في حصول الفعل الإجرامي كانت مرتفعة وبدرجة عالية، وقد احتلّ بعدها دور الضحية الاستفزازي للمجرم المرتبة الأولى، وفي المرتبة الثانية دور طبيعة سلوك الضحية وتأثيرها على دوره في وقوعه كضحية، ثم يلي ذلك المتغيرات الشخصية للضحية، وفي المرتبة الأخيرة سماته الشخصية.

دراسة الجروي (2011)، بعنوان "العوامل الاجتماعيّة والثقافيّة المؤدية لظاهرة ابتزاز المرأة".

هدفت الدّراسة إلى التعرف على أهم العوامل الاجتماعيّة والثقافيّة المؤدية لظاهرة ابتزاز المرأة في المجتمع السعوديّ، الكشف عن دوافع وطرق الابتزاز، التعرف على خصائص وسمات اللواتي يتعرضن للابتزاز والآثار المترتبة عليه، استعانت الباحثة في منهج تحليل المضمون من خلال (15) سجل من سجلات اللواتي تعرضن لجرائم الابتزاز الإلكترونيّ، وتمّ تحويلهن إلى مؤسسة آسية ليكونوا من ضمن برنامج الحماية من الابتزاز، من ثم قامت الباحثة بإعداد دليل لدراسة الحالة، من أهم نتائج الدّراسة: من أهم دوافع الابتزاز لدى المبتز هو من إشباع رغباته الجنسيّة، من أكثر أنواع الابتزاز انتشاراً (الجنسي، والنفسي، والمادي، والعاطفي)، من أهم العوامل المؤدية إلى ظاهرة الابتزاز هي ضعف الوازع الديني، والتفكك الأسري، والفراغ العاطفيّ، ووقت الفراغ.

دراسة الخمشي (2010)، بعنوان " الآثار الاجتماعيّة السلبية لاستخدام الفتاة مرحلة المراهقة للإنترنت".

هدفت الدّراسة إلى معرفة واقع استخدام الفتيات المراهقات للإنترنت ، إضافة إلى تحديد أهم الآثار الاجتماعيّة السلبية على الفتاة وأسررتها ومجتمعها، استخدمت الباحثة منهج المسح الاجتماعيّ، إضافة إلى استبانة من إعدادها، وتكوّنت عينة الدّراسة من (250) فتاة تمّ انتقائهن بالطريقة العشوائية. لخصت الدّراسة إلى العديد من النتائج لعل من أهمها: شعور الفتاة بأنها غير راضية عن حياتها ومظلومة ممّا يؤدي إلى زيادة استخدامها للإنترنت، لينتج عنه تدنٍ في التحصيل الدراسيّ.

دراسة الحمصي (2009)، بعنوان " إدمان الإنترنت عند الشباب وعلاقته بمهارات التواصل الاجتماعيّ، دراسة ميدانية على عيّنة من طلاب جامعة دمشق".

هدفت الدّراسة إلى دراسة ظاهرة إدمان الإنترنت لدى الشباب ومدى تأثيرها على مهارات التواصل الاجتماعيّ لديهم، استخدم الباحث منهج التحليل الوصفي، حيث تكوّنت أدوات الدّراسة من مقياس إدمان الإنترنت إعداد يونغ، ومقياس العلاقات الاجتماعية للحاج، ومن أهم نتائج الدّراسة: وجود علاقة بين مهارات التواصل الاجتماعيّ وإدمان الإنترنت تبعا للعديد من المتغيرات التي تؤثر على طبيعة الإدمان، حيث وجد أنّ الفتيات لديهن قابلية للإدمان أكثر من الشباب.

دراسة كردي (2009)، بعنوان " الاكتئاب والذكاء الانفعالي لدى عيّنة من مدمنات الشبكة العنكبوتية - دراسة وصفية مقارنة ".

هدفت الدّراسة إلى تحديد الفروق في الاكتئاب والذكاء الانفعالي بين طالبات الجامعة مدمنات الشبكة المعلوماتية وغير المدمنات في مدينة الطائف، واستخدم الباحث المنهج التجريبي من خلال تقسيم عيّنة الدّراسة إلى مجموعة تجريبية ومجموعة ضابطة، تألفت عيّنة الدّراسة من (100) طالبة من مدمنات الشبكة و(100) طالبة من غير المدمنات على الشبكة العنكبوتية. في حين أنّ أدوات الدّراسة هي مقياس إدمان الشبكة العنكبوتية ليونغ، ومقياس عزب لتشخيص إدمان الشبكة المعلوماتية، كما استخدم مقياس الاكتئاب ومقياس الذكاء الانفعاليّ. أثبتت النتائج أنّ هناك فرقا ذا دلالة في الاكتئاب بين المدمنات وغير المدمنات يساوي (10،68) أي أنّ الطالبات المدمنات أكثر اكتتابا من الطالبات غير المدمنات، كما وأظهرت فروقا دالة في الذكاء الانفعالي بين المدمنات وغير المدمنات يساوي (11،94) أي غير المدمنات أكثر ذكاء عاطفي من المدمنات على الشبكة العنكبوتية.

2.4.2 الدراسات الأجنبية:

دراسة (Catalan, and Zych, and Ruiz, and Llorent, 2017)، بعنوان " الضحية من خلال الجرائم الإلكترونية(البطجة والتسلط الإلكتروني): الذكاء العاطفي، وشدت الإيذاء واستخدام التكنولوجيا في أنواع مختلفة من الضحايا".

هدفت الدراسة التعرف إلى الأنواع المختلفة للجرائم الإلكترونية وما ينتج عنها من ضرر على الضحية وعلاقته بالذكاء العاطفي لديهم، استخدام الباحث المنهج الوصفي، وتكوّن مجتمع الدراسة من طلاب (22) مدرسة ثانوية في محافظة أندلسية في إسبانيا، تم اختيار عينة الدراسة بطريقة عشوائية حيث تكوّنت من (2139) طالبا وطالبة، وأعمارهم ما بين (11-19) سنة، توصلت الدراسة إلى نتائج مفادها أنّ الضحايا الذين يقعون ضحايا في الحياة الواقعية هم أكثر عرضة لأنّ يكونوا ضحايا للجرائم الإلكترونية، وأنّ الذكاء العاطفي قد يحمي الأولاد من الوقوع كضحايا بالعالم الافتراضي والواقعي.

دراسة (Sharma and Prakash, and Sengar, and Chaudhury, and Singh, 2015) بعنوان "العلاقة بين الذكاء العاطفي والسلوكي الإجرامي - دراسة بين المجرمين المدانين".

هدفت هذه الدراسة إلى: تقييم العلاقة بين الذكاء العاطفي والسلوك الإجرامي، وتكوّن مجتمع الدراسة من (202) مبحوث، منهم (101) مدان بارتكاب جريمة مثل القتل والاغتصاب، و (101) كانوا مجرمين مدانين بجرائم خفيفة وعادية، استخدم الباحث المنهج التجريبي، أخذت عينة بالطريقة الغرضية لتتكون المجموعة الثانية من السجناء العاديين من بيرسي، هوتار، رانتشي والمناطق المجاورة، كانت كلتا المجموعتين تتطابقان مع العمر والجنس والتعليم والمهنة والحالة الاجتماعية، تمّ تقييم جميع المشاركين من خلال استبانة الصحة العامة ومقياس مانغال للذكاء العاطفي، من أهم نتائج هذه الدراسة: حصلت مجموعة المجرمين المدانين بجرائم القتل والاغتصاب على درجات أقلّ بكثير في جميع مجالات الاستبانة مثل: الوعي داخل الذات (المشاعر الخاصة)، التوعية بين الأفراد (عواطف أخرى)، إدارة داخل الذات (المشاعر الخاصة) إدارة العلاقات الشخصية (الآخرين المشاعر)، والحاصل العاطفي الكلي في مقارنة بنظرائهم العاديين.

دراسة (Elipe, Merchan, and Ortega, 2015) بعنوان " الذكاء العاطفي المتصور كمتغير وسيط بين الجرائم الإلكترونية وتأثيرها العاطفي".

الهدف من هذه الدراسة هو تحليل العلاقة بين الذكاء العاطفي المتصور والتأثير العاطفي للجريمة الإلكترونية، وتكوّن مجتمع الدراسة من (636) طالبا جامعيًا من جامعتين في جنوب إسبانيا، واستخدام الباحث المنهج الوصفي التحليلي، واستخدم الباحثان ثلاثة استبانات للتقرير الذاتي "استبانة مشروع التدخل في مجال الجرائم الإلكترونية في أوروبا"، و "مقياس التأثير العاطفي للجرائم

الإلكترونية"، و"ميتا-مود للمهارات-24"، ومن أهم نتائج هذه الدراسة: تأثير الجرائم الإلكترونية على الفرد في العديد من المجالات مثل: الأداء الأكاديمي، الاندماج الاجتماعي، احترام الذات، مما ينتج عنها مشاعر تتراوح بين الغضب والحزن لمشاكل أكثر تعقيدا مثل الاكتئاب، اختلاف تأثير الضحايا فيما بينهم ترجع هذه الاختلافات إلى بعض الخصائص الشخصية، أنّ الذكاء العاطفي يؤثر على العلاقة بين الجرائم الإلكترونية والتأثير العاطفي على الضحايا.

دراسة (Megreya, 2014)، بعنوان "الذكاء العاطفي والسلوك الجنائي".

هدفت الدراسة إلى معرفة العلاقة بين الذكاء العاطفي والسلوك الإجرامي، تكون مجتمع الدراسة من (200) ذكر مصري، تكوّنت عيّنة الدراسة من (100) ذكر جاني و(100) ذكر من غير الجناة، استخدمت الدراسة المنهج التجريبي، وأداة الاستبانة المكونة من اختبار الذكاء العاطفي لجمع البيانات، من أهم نتائج الدراسة أن الجناة الذين يقومون بعدوان مباشر انخفض لديهم مستوى الذكاء العاطفي، بينما الجناة الذين يقومون بالقيام بارتكاب جريمتهم بشكل غير مباشر يتمتعون بمستوى ذكاء عاطفي أكبر، وبالإمكان تخفيض السلوك الإجرامي من خلال تحسين قدرات الذكاء العاطفي مثل: إدارة الغضب والانفعالات، وغير الجناة يتمتعون بمستوى ذكاء عاطفي أكبر من الجناة في الدراسة لأنهم قادرون على فهم ذاتهم، وفهم الآخرين والتحكم في ذاتهم وانفعالاتهم.

دراسة (Ojedokun, and Idemudia, 2013)، بعنوان "الدور المعتدل للذكاء العاطفي بين العوامل الشخصية والجرائم الإلكترونية(البلطجة الإلكترونية) في العديد من مجتمعات الطلاب".

هدفت الدراسة التعرف إلى البحث عن الدور المعتدل للذكاء العاطفي في العلاقة ما بين العوامل الشخصية مثل الأمراض الذهانية والعصبية والميل لارتكاب الجرائم الإلكترونية، تم تطبيق الدراسة في الجامعات النيجيريا حيث تكوّنت عيّنة الدراسة من (198) أنثى جامعية و(199) ذكرا جامعيًا، تم استخدام أداة الاستبانة لجمع البيانات، استخدم الباحث المنهج الكمي التحليلي، ومن أهم نتائج الدراسة: أنّ الذكاء العاطفي قادر على التأثير على العوامل الشخصية للأفراد وميلهم لارتكاب الجرائم الإلكترونية، وأنّ من يقوم بارتكاب الجرائم الإلكترونية يتميز بتدني مستوى الذكاء العاطفي وارتفاع في مستويات الأمراض الذهانية والعصبية (أي العوامل الشخصية).

دراسة (Hampson,2012)، بعنوان " دور الذكاء العاطفي في النشاط الإجرامي للشباب المشاركين في خدمة ليدز للشباب المخالفة".

هدفت الدراسة التعرف إلى تحديد إذا ما كان هناك ارتباط بين الشباب الأذكياء عاطفياً بجوانبهم المختلفة من الإساءة، تمّ استخدام "نموذج ماير وسالوفي" للحصول على البيانات والمعلومات، استخدام الباحث المنهج الوصفي، تكوّن مجتمع الدراسة من (100) شاب يتلقون أوامر الإشراف من خدمة ليدز للشباب الذين ارتكبوا جنح وجرائم مختلفة، تمت مقابلة (13) منهم لاكتساب مزيد من التبصر في عواطفهم، والتحقق من موثوقية وصلاحيّة النموذج بالنسبة للمجرمين الشباب، ومن أهم نتائج الدراسة هناك ضرورة لدراسة الذكاء العاطفي في الجرائم فهو يتيح فرصة للتعاطف مع الضحايا، يجب أن يكون هناك فرصة للشباب المشتركين في خدمة ليدز لتطوير الذكاء العاطفي لديهم لكي يتمكنوا من تقدير مشاعر الآخرين، وفهم عواطفهم.

3.4.2 التعقيب على الدراسات السابقة وذات العلاقة:

بعد استعراض الدراسات السابقة وذات العلاقة التي تناولت الذكاء العاطفي والفعل الإجرامي المتمثل في الجرائم الإلكترونية ونخص بالذكر الابتزاز الإلكتروني، وجد أنّ هناك مجموعة من الاختلافات ما بين الدراسة الحالية والدراسات التي أجريت داخل الدول العربية وأخرى في دول أجنبية، حيث وجد أنّ معظمها يسلط الضوء على الذكاء العاطفي لكن بطرق وأساليب مختلفة، حيث إنّها تناولت الذكاء العاطفي بمرادفاته الذكاء الانفعالي، والذكاء الوجداني تبعاً لمتغيرات نفسية واجتماعية وأمنية مختلفة، لكن دون الأخذ بعين الاعتبار متغير جريمة الابتزاز الإلكتروني والربط بينه وبين الذكاء العاطفي خاصة في الدراسات العربية، هذا ما توضحه هذه الدراسة، بالإضافة إلى قلة البحوث التي تدرس جانب الضحية التي يقع عليها جريمة الابتزاز الإلكتروني، وما هو دورها في ارتكاب الجريمة، حيث أنّه قبل ظهور علم الضحايا لم يكن في وسع العلماء تحديد دور الضحية في حدوث الفعل الإجرامي بحقهم، من هنا جاءت ضرورة النظر إلى الحدث الإجرامي كعملية تفاعلية بين الضحية والجاني لتحديد دور الضحية والعوامل المحيطة فيه أثناء حدوث الجريمة وبعد انتهائها.

اتفقت الدراسة الحالية مع دراسة كلّ من المحمود (2014)، الخليوي (2014)، الشمراني (2011) ، من ناحية الأهداف حيث ركزت على دور مواقع التواصل الاجتماعي في تسهيل جريمة الابتزاز

الإلكترونيّ للمبتز تهديد، وسهولة التواصل والتعارف وإقامة علاقات محرمة بين المبتز والفتاة، إضافة كونها تستخدم من قبل الجاني للابتزاز والتهديد والتشهير إذا لم تستجب الضحية له.

انفقت الدّراسة الحالية مع دراسة الحقباني (2013) حيث ركزت النتائج على ضرورة توافر المهارات العامة اللازمة للبحث والتحقيق في الجرائم المعلوماتية، كون هذا يساعد في تحقيق العدالة بالقبض على الجاني ومعاقبته بشكل رادع حتى لا يعود إلى الفعل مرة أخرى.

انفقت الدّراسة الحالية مع دراسة Elipe, Merchan ,and, Ruiz,Casas (2015) بحيث ركزت على تأثير الجرائم الإلكترونيّة على الفرد في العديد من المجالات مثل: الاندماج الاجتماعي، واحترام الذات، ممّا ينتج عنها مشاعر تتراوح بين الغضب والحزن والاكتئاب.

انفقت الدّراسة الحالية مع دراسة الخمشي (2010)، كردي(2009)، Catalan, and Zych, and Ruiz, and Llorent, (2017)، التي أشارت إلى شعور الفتاة بأنها غير راضية عن حياتها ورغبتها في الحصول على العاطفة وسد الفراغ الذي تعيشه، يؤدي إلى زيادة استخدامها للإنترنت ومواقع التواصل الاجتماعي، الأمر الذي يزيد من احتمالية أن تكون ضحية للابتزاز الإلكترونيّ فيما بعد، وأن الذكاء العاطفيّ قد يحمي الأفراد من الوقوع كضحايا بالعالم الافتراضي والواقعي.

في حين تتفق دراسات Megreya (2013)، Ojedokun, and Idemudia (2014)، Hampson (2012)، مع الدّراسة الحالية حيث ركزت على الجاني الذي من يقوم بارتكاب الجرائم الإلكترونيّة غير المنظمة يتميز بتدني مستوى الذكاء العاطفيّ، وضرورة دراسة الذكاء العاطفيّ في الجرائم فهو يتيح فرصة للتعاطف مع الضحايا، لكي يتمكنوا الجناة من تقدير مشاعر الآخرين، وفهم عواطفهم.

انفقت الدّراسة الحالية مع دراسة المطيري(2015) (النصر، 2017) التي ركزت على وجود فجوة تشريعية بين دول العالم فيما يتعلق بمكافحة جرائم الإلكترونيّ ممّا أدى إلى زيادة هذه الجرائم، وصعوبة تتبع أثر الجاني إذا كان خارج الحدود الجغرافية بسبب اختلاف الجوانب الإجراميّة في العالم واختلاف دوافع وأساليب الجاني، وأنّ مدى انتشار جريمة الابتزاز الإلكترونيّ عبر الشبكات الإلكترونيّة كان مرتفع، كذلك ارتفاع مستوى المعوقات التي تواجه المحققين أثناء التحقيق في جريمتي الابتزاز والتحرش الإلكترونيّ.

اتفقت دراسة كلٍّ من المحمود (2014)، الخليوي (2014)، الشمراني(2011)، الحمصي (2009) مع الدّراسة الحالية من ناحية استخدامهم المنهج الوصفي، لكن هناك اختلاف في مجتمع الدراسة، بينما تختلف الدّراسة الحالية عن دراسة المحمود (2014)، بن النحيت (2016)، الكردي (2009) في المنهج المستخدم.

تمّ الاستفادة من هذه الدراسات في بناء أداة الدّراسة الاستبانة في الجزء المتعلق بجرائم الابتزاز الإلكترونيّ مع دراسة Elipe, Merchan, and Sharma et al. (2015)، ودراسة Ortega (2015)، كذلك دراسة النصر (2017)، أمّا فيما يتعلق في الجزء الخاص بالذكاء العاطفيّ في الاستبانة تتفق هذه الدّراسة الحالية مع دراسة Hampson (2012) حيث تمّ الاستعانة بنموذج ماير وسالوفي (1990) لبناء أداة الاستبانة.

وقد تميزت الدّراسة الحالية عن الدراسات السابقة وذات العلاقة بما يلي:

- تكوّن مجتمع الدّراسة من ضحايا جرائم الابتزاز الإلكترونيّ وهو مجتمع حقيقي لكلا الجنسين.
- استخدمت الباحثة المنهج الوصفيّ في دراستها، واستخدمت أداتين لجمع المعلومات على خلاف غالبية الدراسات السابقة وذات العلاقة.
- استخدمت الباحثة العيّنة القصدية الغرضيّة، وهي عيّنة تحقق الغرض من الدراسة.
- ناقشت الدّراسة الحالية الذكاء العاطفيّ وعلاقته بممارسة جرائم الابتزاز الإلكترونيّ لدى عيّنة من الضحايا.
- توصلت الدّراسة الحالية إلى العديد من النتائج والتوصيات التي تخص جميع شرائح المجتمع الممثلة بالجهات المختصة، ومؤسسات المجتمع المحلي، والأفراد.

الفصل الثالث

الطريقة والإجراءات

يتناول هذا الفصل وصفا مفصلا للطريقة التي تمّ اتباعها لتنفيذ الدراسة، حيث سيتم الحديث عن الطريقة والإجراءات التي تمت لإتمامها من حيث، وصف مجتمع الدراسة، وتحديد عينة الدراسة، وأداة الدراسة (الاستبانة)، والتأكد من صدقها وثباتها، والأساليب الإحصائية التي استخدمت في معالجة النتائج، وفيما يلي وصف لهذه الإجراءات.

3 . 1 منهج الدراسة:

من أجل تحقيق أهداف الدراسة تمّ استخدام المنهج الوصفي بشقيه الكمي من خلال الاستعانة بالاستبانة والنوعي من خلال المقابلة، حيث يعرف المنهج الوصفي بأنه المنهج الذي يدرس ظاهرة أو حدثا أو قضية موجودة حاليا يمكن الحصول منها على معلومات تجيب عن أسئلة البحث دون تدخل أحد، إذ يتم من خلال هذا المنهج وصف الظاهرة موضوع الدراسة، وتحليل بياناتها، وبيان العلاقة بين مكونات والآراء التي تطرح حولها، والعمليات التي تتضمنها والآثار التي تحدثها، وهو أحد أشكال التحليل والتفسير العلمي المنظم لوصف الظاهرة أو المشكلة، وتصنيفها وتحليلها وإخضاعها للدراسات الدقيقة بالفحص والتحليل.

3.2 مجتمع الدراسة:

تألف مجتمع الدراسة من جميع ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية من بداية شهر (1) حتى نهاية شهر (7) من العام 2019 البالغ عددهم (208) ضحية حسب إحصائيات كلّ من (وحدة الجرائم الإلكترونية، ووحدة حماية الأسرة) في جهاز الشرطة الفلسطينية، و(نيابة الجرائم

الإلكترونية) في النيابة العامة، إضافة إلى (5) موظفين عاملين مقسمين على النحو الآتي: (2) وحدة الجرائم الإلكترونية، (2) وحدة حماية الأسرة، (1) نيابة الجرائم الإلكترونية.

3 . 3 عينة الدراسة:

اشتملت عينة الدراسة على (73) استبانة حيث تشكل نسبته (35.1%) من مجتمع الدراسة تم اختيارهم بطريقة قصدية غرضية من مجتمع الدراسة، علماً بأن الاستبيانات التي تم توزيعها بلغت (78)، تم إتلاف واستبعاد (5) استبانات لعدم صلاحيتها للتحليل، كذلك تم عمل (5) مقابلات مع موظفي الوحدات والنيابة للحصول على نتائج قد يكون لها دور كبير في تدعيم نتائج الاستبانة بشكل علمي أفضل وأدق.

4 . 3 وصف متغيرات أفراد العينة:

جدول رقم (1.3): توزيع أفراد عينة الدراسة الذين تم توزيع الاستبانة عليهم حسب متغيرات الدراسة.

المتغير	المستوى	العدد	النسبة المئوية
الجنس	ذكر	30	41.1
	أنثى	43	58.9
المستوى التعليمي	لا يقرأ ولا يكتب	1	1.4
	ابتدائي	2	2.7
	إعدادي	4	5.5
	ثانوي	18	24.7
	دبلوم	9	12.3
	بكالوريوس	31	42.5
	دراسات عليا فما أعلى	8	11.0
	مكان السكن	قرية	39
مخيم	11	15.1	
مدينة	23	31.5	
العمر	من 18 - أقل من 23 سنة.	13	17.8
	من 23 - أقل من 28 سنة.	15	20.5

19.2	14	من 28- أقلّ من 33 سنة.	
9.6	7	من 33- أقلّ من 38 سنة.	
16.4	12	من 38- أقلّ من 43 سنة.	
16.4	12	43 فما فوق.	
76.7	56	يعمل/تعمل	الوظيفة
20.5	15	لا يعمل/لا تعمل	
2.7	2	طالب/طالبة	
39.7	29	من 1450- أقلّ من 2450 شيكل.	مستوى الدخل
28.8	21	من 2450- أقلّ من 3450 شيكل.	
5.5	4	من 3450- 4450 شيكل.	
26.0	19	4450 شيكل فأكثر.	
27.4	20	أعزب/عزباء .	الحالة الاجتماعية
69.9	51	متزوج/متزوجة.	
1.4	1	أرمل/أرملة .	
1.4	1	معلق/معلقة.	
21.9	16	لم يجب	معدل الاستخدام لمواقع التواصل الاجتماعي
23.3	17	3 ساعات فأقل	
32.9	24	من 4-6 ساعات	
21.9	16	7 ساعات فأكثر	

5.3 أداة الدراسة:

من أجل بناء الاستبانة الخاصة بالدراسة تحديداً الجزء الخاص بالذكاء العاطفيّ تمّ الاستعانة بنموذج ماير وسالوفي (1990)، أمّا فيما يخص بجرائم الابتزاز الإلكترونيّ، فقد تمّ الاستعانة بدراسة (Sharma et al., 2015) ودراسة (Elipe, Merchan ,and Ortega, 2015)، كذلك دراسة (النصر، 2017)، حيث تمّ بناء الاستبانة بصورتها الأولية انظر/ي ملحق رقم(1)، من ثمّ عرضت على مشرفة الدراسة، ثم بعد ذلك تمّ عرضها على مجموعة من المحكمين من ذوي الخبرة انظر/ي

ملحق رقم (3)، لإبداء الرأي في فقرات الاستبانة من حيث: مدى وضوح لغة الفقرات وسلامتها لغوياً، ومدى شمول الفقرات للجانب المدروس، وإضافة أي معلومات أو تعديلات أو فقرات يرونها مناسبة، ووفق هذه الملاحظات تم إخراج الاستبانة بصورتها النهائية انظر/ي ملحق رقم (2).

وتكونت الاستبانة من قسمين رئيسيين، القسم الأول: البيانات الديمغرافية، والقسم الثاني: تكون من مجالات الدراسة، وتفرع عنه جزئين: الجزء الأول: الذكاء العاطفي، والجزء الثاني: ممارسة الجرائم الإلكترونية.

إضافة إلى أنه تم بناء أداة المقابلة للموظفين العاملين في وحدتي الجرائم الإلكترونية ووحدة حماية الأسرة لتدعيم نتائج أداة الاستبانة، ثم بعد ذلك تم عرضها على مشرفة الرسالة لتحكيمها من ثم استخدامها للبحث.

1.5.3 صدق الأداة:

تم التحقق من صدق الأداة أيضاً بحساب معامل الارتباط بيرسون لفقرات الاستبانة مع الدرجة الكلية للأداة، واتضح وجود دلالة إحصائية في جميع فقرات الاستبانة ويدل على أن هناك اتساقاً داخلياً بين الفقرات، والجداول وفق الأرقام التالية تبين ذلك: (2.3) (3.3) (4.3) (5.3) (6.3)

جدول رقم (2.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات مستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.5260**	0.000	15	0.455**	0.000	29	0.627**	0.000
2	0.5420**	0.000	16	0.312**	0.007	30	0.526**	0.000
3	0.422**	0.000	17	0.423**	0.000	31	0.676**	0.000
4	0.381**	0.001	18	0.514**	0.000	32	0.628**	0.000
5	0.325**	0.005	19	0.369**	0.001	33	0.469**	0.000
6	0.4850**	0.000	20	0.503**	0.000	34	0.433**	0.000
7	0.4960**	0.000	21	0.542**	0.000	35	0.649**	0.000
8	0.538**	0.000	22	0.294*	120.0	36	0.497**	0.000
9	0.459**	0.000	23	0.506**	0.000	37	0.486**	0.000
10	0.4690**	0.000	24	0.412**	0.000	38	0.398**	0.000
11	0.348**	0.003	25	0.501**	0.000	39	0.591**	0.000
12	0.343**	0.003	26	0.445**	0.000	40	0.300**	100.0
13	0.483**	0.000	27	0.641**	0.000	41	0.607**	0.000
14	0.666**	0.000	28	0.577**	0.000			

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

جدول رقم (3.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.

رقم م	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية
1	0.554**	0.000	7	0.712**	0.000	13	0.655**	0.000
2	0.566**	0.000	8	0.689**	0.000	14	0.731**	0.000
3	0.795**	0.000	9	0.615**	0.000	15	0.755**	0.000
4	0.751**	0.000	10	0.601**	0.000	16	0.831**	0.000
5	0.724**	0.000	11	0.620**	0.000	17	0.749**	0.000
6	0.731**	0.000	12	0.675**	0.000			

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

جدول رقم (4.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني من وجهة نظر الضحايا.

رقم	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية
1	0.324**	50.00	8	0.493**	0.000	15	0.502**	0.000
2	0.550**	0.000	9	0.586**	0.000	16	0.782**	0.000
3	0.500**	0.000	10	0.440**	0.000	17	0.721**	0.000
4	0.685**	0.000	11	0.463**	0.000	18	0.758**	0.000
5	0.553**	0.000	12	0.495**	0.000	19	0.751**	0.000
6	0.606**	0.000	13	0.338**	30.00	20	0.772**	0.000
7	0.351**	20.00	14	0.675**	0.000	21	0.753**	0.000

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

جدول رقم (5.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.

رقم	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية	رقم	قيمة R	الدالة الإحصائية
1	0.305**	90.00	7	0.645**	0.000	13	0.616**	0.000
2	0.467**	0.000	8	0.414**	0.000	14	0.494**	0.000
3	0.342**	30.00	9	0.413**	0.000	15	0.684**	0.000
4	0.408**	0.000	10	0.641**	0.000	16	0.622**	0.000
5	0.524**	0.000	11	0.641**	0.000			
6	0.527**	0.000	12	0.577**	0.000			

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

جدول رقم (6.3): نتائج معامل ارتباط بيرسون (Pearson Correlation) لمصفوفة ارتباط فقرات الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.

الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية	الرقم	قيمة R	الدالة الإحصائية
1	0.513**	0.000	6	0.632**	0.000	11	0.674**	0.000
2	0.666**	0.000	7	0.461**	0.000	12	0.791**	0.000
3	0.699**	0.000	8	0.693**	0.000	13	0.852**	0.000
4	0.733**	0.000	9	0.712**	0.000	14	0.637**	0.000
5	0.690**	0.000	10	0.736**	0.000	15	0.555**	0.000

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

2.5.3 ثبات أداة الدراسة:

تم التحقق من ثبات الأداة من خلال حساب ثبات الدرجة الكلية لمعامل الثبات لمجالات الدراسة حسب معادلة الثبات كرونباخ ألفا، كانت الدرجة الكلية تشير إلى تمتع هذه الأداة بثبات يفي بأغراض الدراسة، الجدول رقم (7.3) يبين معامل الثبات للمجالات.

جدول رقم (7.3): نتائج معامل الثبات للمجالات

المجالات	معامل الثبات
مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني	0.862
الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني	0.930
الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني	0.903
الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز الإلكتروني	0.781
الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا	0.911
الدرجة الكلية لممارسة جرائم الابتزاز الإلكتروني	0.955

3 . 6 إجراءات الدراسة:

تمت إجراءات الدراسة وفق الخطوات الآتية:

1. تم بناء الأدب النظري للدراسة من خلال الاطلاع على الكتب والمصادر والدراسات السابقة، كذلك من خلال الاطلاع على الوثائق من الجهات المختصة(كوحدة الجرائم الالكترونية ووحدة حماية الاسرة في الشرطة الفلسطينية، ووحدة الجرائم الالكترونية في النيابة العامة).
2. تم بناء استبانته الدراسة في مرحلتها الاولى، ثم عرضها على المحكمين من ذوي الخبرة والاختصاص لإبداء الرأي والتعديل بما يتناسب مع متطلبات الدراسة، وتم اعتمادها في المرحلة النهائية(ملحق2).
3. تم بناء مقابلة الدراسة، وقام المشرف بالاطلاع عليها وتعديلها بما يتناسب مع الدراسة، ثم توزيعها على افراد وحدتي الجرائم الالكترونية في الشرطة والنيابة العامة، ووحدة حماية الاسرة في الشرطة الفلسطينية.
4. تم جمع الاستبانات بعد توزيعها على الضحايا، حيث تم استعادة (73) من أصل (78) استبانته، وهي التي تم تحليلها لاستخراج النتائج.
5. تم تحليل البيانات الخاصة بالاستبانته، والمقابلة، ثم العمل على مناقشتها وربطها بالدراسات السابقة.

3 . 7 المعالجة الإحصائية:

تم جمع الاستبيانات والتأكد من صلاحيتها للتليل ثم تم ترميزها من خلال إعطائها أرقاماً معينة، ذلك تمهيدا لإدخال بياناتها إلى جهاز الحاسوب الآلي لإجراء المعالجات الإحصائية المناسبة، وتحليل البيانات وفقا لأسئلة الدراسة وبيانات الدراسة، حيث تمت المعالجة الإحصائية للبيانات باستخراج المتوسطات الحسابية والانحرافات المعيارية لكل فقرة من فقرات الاستبانة، واختبار (t- test)، واختبار تحليل التباين الأحادي (one way ANOVA)، ومعامل ارتباط بيرسون، ومعادلة الثبات كرونباخ ألفا (Cronbach Alpha)، وذلك باستخدام الرزم الإحصائية (SPSS) (Statistical Package For Social Sciences).

الفصل الرابع

نتائج الدراسة

1.4 مقدمة:

تضمن هذا الفصل عرضاً لنتائج الدراسة، التي تمّ التوصل إليها عن موضوع الدراسة حول " الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عيّنة من الضحايا في الضفة الغربية " وبيان أثر كلّ من المتغيرات من خلال استجابة أفراد العيّنة على أداة الدراسة، وتحليل البيانات الإحصائية التي تمّ الحصول عليها، وحتى يتم تحديد درجة متوسطات استجابة أفراد عيّنة الدراسة تمّ اعتماد الدرجات التالية:

الدرجة	مدى متوسطها الحسابي
منخفضة	2.33 فأقل
متوسطة	3.67-2.34
عالية	3.68 فأعلى

4 . 2 نتائج أسئلة الدراسة:

1.2.4 النتائج المتعلقة بالسؤال الأول:

ما مستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية؟
للإجابة عن هذا السؤال تم احتساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني، الجدول رقم (1.4) يبين ذلك:

جدول رقم (1.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لمستوى الذكاء العاطفي لدى عينة من ضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية.

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	أحسن الظن بالآخرين	3.64	1.135	متوسطة
2	أعبر عن مشاعري بدقة	3.64	1.005	متوسطة
3	إذا تعرضت لمحنة ما أخففت عنها بنفسك	3.71	0.920	عالية
4	استطيع أن أحدد العديد من الأشياء التي (اشمئز، أفرغ) منها	4.05	0.848	عالية
5	أدرك مشاعري كلما تغيرت	3.96	0.904	عالية
6	لدي مشاعر سلبية	2.62	1.049	متوسطة
7	ليس لدي الشجاعة لأرد الإهانة بمنزلها	2.64	1.159	متوسطة
8	أجد صعوبة في التعبير عن أفكاري	3.03	1.093	متوسطة
9	أتردد في توجيه اللوم لشخص يسيء للآخرين	2.84	1.155	متوسطة
10	أنا جدير باحترام الآخرين	4.16	0.764	عالية
11	أنا جدير بحب الآخرين	4.18	0.714	عالية
12	عادة أستطيع أن أفعل ما احتاجه عاطفياً بإرادتي	3.92	0.862	عالية
13	أعتقد أنني قذرة صالحة	3.85	0.861	عالية
14	أنا أقل أهمية من الآخرين	3.58	1.246	متوسطة
15	في المواقف الاجتماعية عندي أفكار مهمة أقولها	3.92	0.894	عالية
16	أتعامل مع الآخرين باحترام متبادل	4.34	0.768	عالية
17	أقبل الواقع كما هو (حلوه، مره)	3.74	0.958	عالية
18	أنا فاشل	3.93	1.217	عالية
19	أستطيع احتواء مشاعر الإجهاد التي تعوق أدائي لمهامي	3.62	0.892	متوسطة
20	أجد صعوبة في أن أبدا أنشطة جديدة بمفردي	2.71	1.099	متوسطة
21	أفضل أن يتخذ الآخرين قراراتي	3.41	1.321	متوسطة
22	أوافق أو أرفض حسب رأي المجموعة	2.89	1.275	متوسطة
23	أتجنب إيذاء مشاعر الآخرين	4.01	0.890	عالية

عالية	1.076	3.70	أنا سعيد في حياتي	24
عالية	0.804	4.27	أفرح لفرح الناس	25
عالية	0.889	4.29	أحزن لحزن الناس	26
متوسطة	1.148	3.29	أشعر بالفشل في علاقتي الاجتماعية	27
متوسطة	1.190	3.16	غيابي لفترة طويلة لا يشعر به من حولي	28
متوسطة	1.009	2.81	لدي قناعة بأن علاقتي مع الآخرين مؤقتة	29
متوسطة	1.052	3.41	إذا تعارضت مصلحتي مع المصلحة العامة أتنازل عن مصلحتي	30
متوسطة	1.160	2.96	أجد صعوبة في التوصل لحل المشكلات التي تواجهني	31
متوسطة	1.029	3.49	أتجنب انفعالات "القلق، الغضب، الخوف" في موقف حلّ المشكلة	32
متوسطة	1.070	2.34	أشعر بان الواقع (زائف، وخداع)	33
متوسطة	1.044	2.66	انا مندفع وراء "أحلامي، خيالاتي"	34
متوسطة	1.161	2.99	انطباعي الأول عن الأشخاص لا يتغير	35
متوسطة	1.294	2.86	كلما ازدادت همومي، أنام لساعات طويلة	36
متوسطة	1.112	2.71	أتعامل مع الشدائد بعصبية	37
متوسطة	1.117	2.88	كثير من تصرفاتي تغضب الآخرين	38
متوسطة	1.061	2.63	أتورط في مجازفات جديدة	39
عالية	1.034	3.77	روحي المعنوية مرتفعة	40
متوسطة	1.248	2.53	تحاصرني الهموم من كل اتجاه	41
متوسطة	0.41105	3.3939	الدرجة الكلية	

يلاحظ من الجدول رقم (1.4) الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني أنّ المتوسط الحسابي للدرجة الكلية (3.39) وانحراف معياري (0.411)، هذا يدل على أن مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني جاء بدرجة متوسطة.

كما وتشير النتائج في الجدول رقم (1.4) أنّ (16) فقرة جاءت بدرجة عالية و(25) فقرة جاءت بدرجة متوسطة. وحصلت الفقرة " أتعامل مع الآخرين باحترام متبادل " على أعلى متوسط حسابي (4.34)،

يليها فقرة " الغض أحزن لحزن الناس " بمتوسط حسابي (4.29). وحصلت الفقرة " أشعر بأن الواقع

(زائف، وخداع) " على أقلّ متوسط حسابي (2.34)، يليها الفقرة " تحاصرني الهموم من كلّ اتجاه "

بمتوسط حسابي (2.53)

2.2.4 النتائج المتعلقة بالسؤال الرئيسي الثاني:

ما واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية؟

للإجابة عن هذا السؤال قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على مجالات الاستبانة التي تعبر عن واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية.

جدول (2.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة لواقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية

الرقم	المجالات	المتوسط الحسابي	الانحراف المعياري	الدرجة
4	الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا	4.2548	0.52709	عالية
3	الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني	4.1233	0.40970	عالية
1	الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني	4.0290	0.67655	عالية
2	الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني	3.9048	0.59600	عالية
	الدرجة الكلية	4.0645	0.39786	عالية

يلاحظ من الجدول السابق الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية أن المتوسط الحسابي للدرجة الكلية (4.06) وانحراف معياري (0.397) وهذا يدل على أن واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية جاء بدرجة عالية.

ولقد حصل مجال الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا على أعلى متوسط حسابي ومقداره (4.25)، ومن ثم مجال الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني بمتوسط حسابي (4.12)، ومن ثم مجال الوسائل

المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني بمتوسط حسابي (4.02)، يليه مجال الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني بمتوسط حسابي (3.90).

1.2.2.4 النتائج المتعلقة بالسؤال الفرعي الأول:

ما هي الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني؟ للإجابة عن هذا السؤال قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني.

جدول (3.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	العلاقات العاطفية	4.34	0.870	عالية
15	أرسال المبتز معلومات خاصة به لكسب ثقة الضحية	4.33	0.914	عالية
5	ابتزاز الضحية بنشر "الصور، المحادثات" الخاصة به على مواقع التواصل الاجتماعي	4.19	1.076	عالية
3	اختراق مواقع التواصل الاجتماعي الخاصة بالضحية للحصول على معلومات خاصة بالضحية	4.14	0.933	عالية
14	عروض الزواج الوهمية	4.14	1.071	عالية
16	اختراق مواقع التواصل الاجتماعي الخاصة بالضحية للحصول على "معلومات، بيانات" خاصة بالضحية	4.12	0.832	عالية
2	استدراج الضحية	4.11	1.008	عالية
8	وعود الضحية بالحصول على علاقة عاطفية يطمح إليها	4.10	0.885	عالية
4	قيام المبتز بانتحال شخصيات أخرى للوصول إلى الضحية	4.08	1.024	عالية
6	استغلال المبتز "لقدراته، مهاراته" العالية في استخدام الشبكة العنكبوتية للقيام في جريمة الابتزاز الإلكتروني	4.08	0.894	عالية
17	قيام المبتز بانتحال شخصيات أخرى للوصول إلى الضحية المناسبة	4.04	0.949	عالية
9	اختيار الضحية المناسبة التي تتمتع بتدني تقدير الذات	3.97	0.942	عالية
7	أرسال المبتز روابط تؤدي إلى اختراق حسابات الضحية للوصول إلى المعلومات الخاصة بها	3.90	1.056	عالية
12	التسلسل الغير مشروع لبيانات المحفوظة على جهاز الضحية الذي تم (تصليحه، ضياعه)	3.81	0.995	عالية
10	استغلال المبتز غياب الرقابة على مواقع التواصل الاجتماعي	3.74	1.093	عالية
11	الدخول إلى حساب الضحية من خلال الهكر	3.74	1.028	عالية
13	استخدام المواقع الإباحية كوسيلة لأغراء الضحية	3.66	1.108	متوسطة
	الدرجة الكلية	4.0290	0.67655	عالية

يلاحظ من الجدول السابق الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني أن المتوسط الحسابي للدرجة الكلية (4.02) وانحراف معياري (0.676) وهذا يدل على أن الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني جاء بدرجة عالية.

كما وتشير النتائج في الجدول رقم (3.4) أن (16) فقرة جاءت بدرجة عالية وفقرة واحدة جاءت بدرجة متوسطة. وحصلت الفقرة " العلاقات العاطفية " على أعلى متوسط حسابي (4.34)، يليها فقرة " إرسال المبتز معلومات خاصة به لكسب ثقة الضحية " بمتوسط حسابي (4.33). وحصلت الفقرة " استخدام المواقع الإباحية كوسيلة لأغراء الضحية " على أقل متوسط حسابي (3.66)، يليها الفقرة " الدخول إلى حساب الضحية من خلال الهكر " والفقرة " استغلال المبتز غياب الرقابة على مواقع التواصل الاجتماعي " بمتوسط حسابي (3.74).

2.2.2.4 النتائج المتعلقة بالسؤال الفرعي الثاني: ما أهم الأسباب التي تؤدي إلى جرائم الابتزاز

الإلكتروني ؟

للإجابة عن هذا السؤال قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني.

جدول (4.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني

الدرجة	الانحراف المعياري	المتوسط الحسابي	الفقرات	الرقم
عالية	0.648	4.49	الاختلاط بأصدقاء السوء	13
عالية	0.814	4.41	ضعف الوازع الديني	8
عالية	0.806	4.36	التفكك الأسري	9
عالية	0.834	4.26	انعدام الرقابة "الذاتية، المجتمعية"	10
عالية	0.953	4.15	ارتفاع نسبة البطالة	1
عالية	0.983	4.08	استخدم الاحتلال في العديد من الأحيان الابتزاز الإلكتروني وسيلة لتحقيق مأربه	7
عالية	0.874	4.01	ضغوط الحياة العامة (الاقتصادية، الاجتماعية، السياسية، الصحية)	3
عالية	0.887	3.93	نمط الحياة التي يتعامل بها الفرد مع الآخرين	12
عالية	1.021	3.89	استفزاز الضحية للمبتز	11
عالية	1.040	3.88	الخوف الذاتي	16
عالية	0.962	3.82	الخوف المجتمعي	15
عالية	1.178	3.79	التحدي بين الشباب	6
عالية	1.017	3.78	عدم القدرة على اختيار جهة الدعم	20
عالية	1.017	3.73	سرعة تنفيذ الجريمة الإلكترونية	5
عالية	1.076	3.70	عدم وجود رقابة حكومية على مواقع التواصل الاجتماعي	14
متوسطة	1.096	3.66	ارتفاع نسبة الثراء لدى طبقة معينة في المجتمع	2
متوسطة	1.145	3.66	عدم الثقة بالأشخاص	19
متوسطة	1.168	3.53	ضعف تنفيذ القوانين الخاصة بالجرائم الإلكترونية	4
متوسطة	1.248	3.48	عدم الثقة بالنيابة	17
متوسطة	1.215	3.48	عدم الثقة بالقضاء	18
عالية	0.59314	3.9041	الدرجة الكلية	

يلاحظ من الجدول السابق الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني أن المتوسط الحسابي للدرجة الكلية (3.90) وانحراف معياري (0.593) وهذا يدل على أن الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني جاء بدرجة عالية.

كما وتشير النتائج في الجدول رقم (4.4) أن (15) فقرة جاءت بدرجة عالية و(5) فقرات جاءت بدرجة متوسطة. وحصلت الفقرة "الاختلاط بأصدقاء السوء" على أعلى متوسط حسابي (4.49)،

ويليها فقرة " ضعف الوازع الديني " بمتوسط حسابي (4.41). وحصلت الفقرة " عدم الثقة بالقضاء " والفقرة " عدم الثقة بالنيابة " على أقل متوسط حسابي (3.48)، يليها الفقرة " ضعف تنفيذ القوانين الخاصة بالجرائم الإلكترونية " بمتوسط حسابي (3.53).

3.2.2.4 النتائج المتعلقة بالسؤال الفرعي الثالث:

ما هي الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني؟
للإجابة عن هذا السؤال قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني.

جدول (5.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة للإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع ضحايا جرائم الابتزاز الإلكتروني

الدرجة	الانحراف المعياري	المتوسط الحسابي	الفقرات	الرقم
عالية	0.783	4.47	جميع إجراءاتها تتم يسرية تامة، ذلك للحفاظ على سمعة الضحية	15
عالية	0.812	4.40	إتباع قانون الجرائم الإلكترونية في فرض العقوبة المناسبة على المبتز	1
عالية	0.858	4.37	تقوم بحملات توعية عن خطورة الابتزاز الإلكتروني	11
عالية	0.773	4.37	تعزيز (التعاون، التنسيق) مع المؤسسات (الدولية، المحلية) المعنية بمكافحة الجرائم الإلكترونية	16
عالية	0.788	4.36	تعمل على وضع خطط لمعالجة جرائم الابتزاز الإلكتروني	12
عالية	0.786	4.27	التأكيد على الضحية بعدم التعاون مع المبتز	13
عالية	0.842	4.23	تحويل الضحية إلى وحدة حماية الأسرة اذا لزم الأمر	14
عالية	0.833	4.21	مساندة ضحايا جريمة الابتزاز الإلكتروني	2
عالية	0.843	4.11	مواجهة المبتز بمحادثات التهديد التي قام بها	9
عالية	0.595	4.08	تحديد نوعية الابتزاز ليتم تحديد الآلية المناسبة للتعامل معه	8
عالية	0.903	4.07	اختراق جهاز المبتز بهدف تدمير كافة (البيانات، المعلومات) التي يبتز بها الضحية	10
عالية	0.857	4.04	تفعيل دور المرشد "الاجتماعي، النفسي" في التعامل مع الضحية	5
عالية	0.897	3.97	توفير رقم موحد للتبليغ عن جرائم الابتزاز الإلكتروني	6
عالية	0.877	3.85	التدخل في سير جريمة الابتزاز الإلكتروني للقبض على المبتز متلبساً أثناء ارتكابه جريمة الابتزاز الإلكتروني	4
عالية	0.950	3.71	استخدام الضحية كأداة للمساعدة في القبض على المبتز	3
متوسطة	1.081	3.47	اللجوء إلى الجهات العشائرية لحل جريمة الابتزاز الإلكتروني بطرق ودية	7
عالية	0.40970	4.1233	الدرجة الكلية	

يلاحظ من الجدول السابق الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني أن المتوسط الحسابي للدرجة الكلية(4.12) وانحراف معياري (0.409) وهذا يدل على أن الإجراءات المتبعة من " نيابة الجرائم الإلكترونية، وحدة حماية الأسرة" للتعامل مع جرائم الابتزاز الإلكتروني جاء بدرجة عالية.

كما وتشير النتائج في الجدول رقم (5.4) أن (15) فقرة جاءت بدرجة عالية وفقرة واحدة جاءت بدرجة متوسطة. وحصلت الفقرة " جميع إجراءاتها تتم بسرية تامة، ذلك للحفاظ على سمعة الضحية " على أعلى متوسط حسابي (4.47)، يليها فقرة " إتباع قانون الجرائم الإلكترونية في فرض العقوبة المناسبة على المبتز " بمتوسط حسابي (4.40). وحصلت الفقرة " اللجوء إلى الجهات العشائرية لحل جريمة الابتزاز الإلكتروني بطرق ودية " على أقل متوسط حسابي (3.47)، يليها الفقرة " استخدام الضحية كأداة للمساعدة في القبض على المبتز " بمتوسط حسابي(3.71).

4.2.2.4 النتائج المتعلقة بالسؤال الفرعي الرابع:

ما هي الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا ؟
للإجابة عن هذا السؤال قامت الباحثة بحساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة على فقرات الاستبانة التي تعبر عن الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.

جدول (6.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا

الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
2	التفكك اسري	4.51	0.648	عالية
1	انتشار الانحراف بين الضحايا والمبتزين	4.45	0.554	عالية
3	الطلاق	4.41	0.742	عالية
4	سلب الموارد المادية للضحية	4.40	0.721	عالية
11	خداع الضحية من خلال مشاعر الحب	4.40	0.759	عالية
5	حدوث خلافات عشائرية عند معرفة المبتز والضحية لبعضهم البعض	4.30	0.794	عالية
9	لجوء المبتز إلى الضغط على الضحية لارتكاب مخالفات (أخلاقية، قانونية)	4.25	0.778	عالية
8	تراجع قوة القيم، لردع السلوك المنحرف في المجتمع	4.21	0.706	عالية
6	تعرض الضحية للقتل من قبل عائلته خوفاً من الفضيحة	4.19	0.844	عالية
10	تدني الكفاءة الشخصية أكثر لدى الضحية في حل مشاكله	4.19	0.844	عالية
13	كره الحياة	4.16	0.943	عالية
12	تراجع ثقة الضحية بنفسه	4.15	0.828	عالية
7	تهديد الأمن العام	4.14	0.918	عالية
15	يتحول مزاج الضحية إلى مزاج حاد يصعب التعامل معه	4.11	0.809	عالية
14	تدني مستوى الذكاء العاطفي لدى الضحية " مع العلم بان الذكاء العاطفي يعني قدرة الفرد على مراقبة مشاعره وانفعالاته الذاتية وانفعالات ومشاعر الآخرين والموازنة بينهما".	3.96	0.873	عالية
	الدرجة الكلية	4.2548	0.52709	عالية

يلاحظ من الجدول السابق الذي يعبر عن المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد

عينة الدراسة على الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا أن المتوسط الحسابي

للدرجة الكلية (4.25) وانحراف معياري (0.527) وهذا يدل على أن الأثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا جاء بدرجة عالية.

كما وتشير النتائج في الجدول رقم (6.4) أن جميع الفقرات جاءت بدرجة عالية. وحصلت الفقرة " التفكك اسري " على أعلى متوسط حسابي (4.51)، يليها فقرة " انتشار الانحراف بين الضحايا والمبتزين " بمتوسط حسابي (4.45). وحصلت الفقرة " تدني مستوى الذكاء العاطفي لدى الضحية " مع العلم بان الذكاء العاطفي يعني قدرة الفرد على مراقبة مشاعره وانفعالاته الذاتية وانفعالات ومشاعر الآخرين والموازنة بينهما" على أقل متوسط حسابي (3.96)، يليها الفقرة " يتحول مزاج الضحية إلى مزاج حاد يصعب التعامل معه " بمتوسط حسابي (4.11).

3.2.4 النتائج المتعلقة بالسؤال الرئيسي الثالث: هل توجد علاقة ذات دلالة إحصائية عند مستوى

الدلالة ($0.05 \geq \alpha$) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا ؟

للإجابة عن هذا السؤال تم تحويله لفرضية التالية:

يوجد علاقة ذات دلالة احصائية عند مستوى الدلالة ($0.05 \geq \alpha$) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا.

تم فحص الفرضية بحساب معامل ارتباط بيرسون والدلالة الاحصائية بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا.

جدول (7.4): معامل ارتباط بيرسون والدلالة الاحصائية للعلاقة بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا

مستوى الدلالة	معامل بيرسون	المتغيرات	
0.596	-0.063	ممارسة جرائم الابتزاز الإلكتروني	مستوى الذكاء العاطفي

يتبين من خلال الجدول السابق أنّ قيمة معامل ارتباط بيرسون للدرجة الكلية (-0.063)، ومستوى الدلالة (0.596)، أي أنه لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا. وبذلك تم رفض الفرضية.

4.2.4 النتائج المتعلقة بالسؤال الرئيسي الرابع:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغيرات الدراسة (الجنس، المستوى التعليمي، مكان السكن، العمر، الوظيفة، مستوى الدخل، الحالة الاجتماعية، معدل استخدام مواقع التواصل الاجتماعي)؟

وللإجابة عن هذا السؤال تم تحويله للفرضيات التالية:

نتائج الفرضية الأولى: "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير الجنس"

تم فحص الفرضية الأولى بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في ممارسة جرائم الابتزاز الإلكتروني حسب لمتغير الجنس.

جدول (8.4): نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني حسب متغير الجنس

الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة "t"	مستوى الدلالة
ذكر	30	4.0368	0.30234	0.494	0.623
أنثى	43	4.0838	0.45531		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكلية (0.494)، ومستوى الدلالة (0.623)، أي أنه لا توجد فروق في ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير الجنس، وبذلك تم رفض الفرضية الأولى.

نتائج الفرضية الثانية: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي " تم فحص الفرضية الثانية تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي.

جدول (9.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي

المستوى التعليمي	العدد	المتوسط الحسابي	الانحراف المعياري
ثانوي فما دون	25	4.0453	0.50698
دبلوم	9	4.4020	0.18426
بكالوريوس فأعلى	39	3.9989	0.31433

يلاحظ من الجدول رقم (9.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (10.4):

جدول(10.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	1.202	2	0.601	4.127	0.020
داخل المجموعات	10.195	70	0.146		
المجموع	11.397	72			

يلاحظ أن قيمة ف للدرجة الكلية(4.127) ومستوى الدلالة (0.020) وهي أقل من مستوى الدلالة ($0.05 \geq \alpha$) أي أنه توجد فروق دالة إحصائياً في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير المستوى التعليمي، وبذلك تم قبول الفرضية الثانية. وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كمايلي:

الجدول (11.4): نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير المستوى التعليمي

المتغيرات	الفروق في المتوسطات	مستوى الدلالة
ثانوي فما دون	-0.35667	0.019
دبلوم	0.04643	0.636
بكالوريوس فأعلى	0.35667	0.019
دبلوم	0.40309	0.006
بكالوريوس فأعلى	-0.04643	0.636
بكالوريوس فأعلى	-0.40309	0.006
دبلوم		

وكانت الفروق بين الدبلوم وقانوني فما دون لصالح الدبلوم، وبين الدبلوم وبكالوريوس فأعلى لصالح الدبلوم.

نتائج الفرضية الثالثة: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن"

تم فحص الفرضية الثالثة تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن.

جدول (12.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن

مكان السكن	العدد	المتوسط الحسابي	الانحراف المعياري
قرية	39	4.0807	0.45481
مخيم	11	4.1083	0.32720
مدينة	23	4.0160	0.32895

يلاحظ من الجدول رقم (10.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (13.4):

جدول(13.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.085	2	0.043	0.264	0.768
داخل المجموعات	11.311	70	0.162		
المجموع	11.397	72			

يلاحظ أن قيمة F للدرجة الكلية (0.264) ومستوى الدلالة (0.768) وهي أكبر من مستوى الدلالة ($0.05 \geq \alpha$) أي أنه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مكان السكن، وبذلك تم رفض الفرضية الثالثة.

نتائج الفرضية الرابعة: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر "

تم فحص الفرضية الرابعة تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر .

جدول (14.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر

العمر	العدد	المتوسط الحسابي	الانحراف المعياري
من 18 - أقل من 23 سنة.	13	3.9796	0.57911
من 23 - أقل من 28 سنة.	15	4.1647	0.35682
من 28 - أقل من 33 سنة.	14	4.1670	0.35288
من 33 - أقل من 38 سنة.	7	4.1387	0.32351
من 38 - أقل من 43 سنة.	12	3.9669	0.35004
43 فما فوق.	12	3.9657	0.34825

يلاحظ من الجدول رقم (14.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (15.4):

جدول (15.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.661	5	0.132	0.825	0.536
داخل المجموعات	10.736	67	0.160		
المجموع	11.397	72			

يلاحظ أن قيمة ف للدرجة الكلية (0.825) ومستوى الدلالة (0.536) وهي أكبر من مستوى الدلالة ($0.05 \geq \alpha$) أي أنه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير العمر، وبذلك تم رفض الفرضية الرابعة.

نتائج الفرضية الخامسة: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير الوظيفة "

تم فحص الفرضية الخامسة بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في ممارسة جرائم الابتزاز الإلكتروني حسب لمتغير الوظيفة.

جدول (16.4): نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني حسب متغير الوظيفة

الوظيفة	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة "ت"	مستوى الدلالة
يعمل / تعمل	56	4.0473	0.37312	0.597	0.552
لا يعمل / لا تعمل	15	4.1167	0.49009		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكلية (0.597)، ومستوى الدلالة (0.552)، أي أنه لا توجد فروق في ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير الوظيفة، وبذلك تم رفض الفرضية الثانية.

نتائج الفرضية السادسة: "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل " تم فحص الفرضية السادسة تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل.

جدول (17.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل

مستوى الدخل	العدد	المتوسط الحسابي	الانحراف المعياري
من 1450 - أقل من 2450 شيكل.	29	4.1729	0.41862
من 2450 - أقل من 3450 شيكل.	21	3.9755	0.42592
من 3450 شيكل فأكثر	23	4.0090	0.32218

يلاحظ من الجدول رقم (17.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل، ولمعرفة دلالة الفروق تم استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (18.4):

جدول(18.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	0.578	2	0.289	1.871	0.162
داخل المجموعات	10.819	70	0.155		
المجموع	11.397	72			

يلاحظ أن قيمة ف للدرجة الكلية (1.871) ومستوى الدلالة (0.162) وهي أكبر من مستوى الدلالة ($0.05 \geq \alpha$) أي أنه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير مستوى الدخل، وبذلك تم رفض الفرضية السادسة.

نتائج الفرضية السابعة: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير الحالة الاجتماعية "

تم فحص الفرضية السابعة بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في ممارسة جرائم الابتزاز الإلكتروني حسب لمتغير الحالة الاجتماعية.

جدول (19.4): نتائج اختبار "ت" للعينات المستقلة لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني حسب متغير الحالة الاجتماعية

الحالة الاجتماعية	العدد	المتوسط الحسابي	الانحراف المعياري	قيمة "ت"	مستوى الدلالة
أعزب/ عزباء .	20	4.1779	0.49579	1.716	0.091
متزوج/ متزوجة.	51	4.0014	0.34118		

يتبين من خلال الجدول السابق أن قيمة "ت" للدرجة الكلية (1.716)، ومستوى الدلالة (0.091)، أي أنه لا توجد فروق في ممارسة جرائم الابتزاز الإلكتروني تعزى لمتغير الحالة الاجتماعية، وبذلك تم رفض الفرضية السابعة.

نتائج الفرضية الثامنة: " توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي "

تم فحص الفرضية الثامنة تم حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي.

جدول (20.4): المتوسطات الحسابية والانحرافات المعيارية لاستجابة أفراد عينة الدراسة لممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي

الانحراف المعياري	المتوسط الحسابي	العدد	معدل الاستخدام لمواقع التواصل الاجتماعي
0.55460	3.8658	16	لم يجب
0.25125	4.0709	17	3 ساعات فأقل
0.29485	4.0374	24	من 4-6 ساعات
0.38812	4.2969	16	7 ساعات فأكثر

يلاحظ من الجدول رقم (20.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي، ولمعرفة دلالة الفروق تم استخدام تحليل التباين

الأحادي (one way ANOVA) كما يظهر في الجدول رقم (21.4):

جدول(21.4): نتائج اختبار تحليل التباين الأحادي لاستجابة أفراد العينة في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي

مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة "ف" المحسوبة	مستوى الدلالة
بين المجموعات	1.514	3	0.505	3.523	0.019
داخل المجموعات	9.883	69	0.143		
المجموع	11.397	72			

يلاحظ أن قيمة ف للدرجة الكلية (3.523) ومستوى الدلالة (0.019) وهي أقل من مستوى الدلالة ($0.05 \geq \alpha$) أي أنه توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني يعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي، وبذلك تم قبول الفرضية الثامنة. وتم فحص نتائج اختبار (LSD) لبيان اتجاه الفروق وهي كمايلي:

الجدول (22.4): نتائج اختبار (LSD) للمقارنات البعدية بين المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حسب متغير معدل الاستخدام لمواقع التواصل الاجتماعي

المتغيرات	الفروق في المتوسطات	مستوى الدلالة
لم يجب	3 ساعات فأقل	0.124
	من 4-6 ساعات	0.165
	7 ساعات فأكثر	0.002
3 ساعات فأقل	لم يجب	0.124
	من 4-6 ساعات	0.781
	7 ساعات فأكثر	0.091
من 4-6 ساعات	لم يجب	0.165
	3 ساعات فأقل	0.781
	7 ساعات فأكثر	0.037
7 ساعات فأكثر	لم يجب	0.002
	3 ساعات فأقل	0.091
	من 4-6 ساعات	0.037

وكانت الفروق بين (7 ساعات فأكثر) و(لم يجب) لصالح (7 ساعات فأكثر)، وبين (7 ساعات فأكثر) و(من 4-6 ساعات) لصالح (7 ساعات فأكثر).

3.4 نتائج المقابلات:

بعد الانتهاء من عمل المقابلات مع 5 من العاملين في وحدة الجريمة الإلكترونية وحماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة، تمّ التوصل إلى النتائج الآتية:

الاسم	العمر	المستوى التعليمي	مكان العمل	دائرة العمل	المسمى الوظيفي	الرتبة	عدد سنوات الخبرة	أماكن العمل السابقة
سونيا خليل عزاب	28	بكالوريوس	الشرطة	وحدة الجرائم الإلكترونية	مهندس-مختبر الأدلة الرقمية	ملازم أول	3	شركة JREX
ديما يوسف عرب	26	بكالوريوس	النيابة العامة	مكتب النائب العام	باحث قانوني نيابة الجرائم الإلكترونية	سنة	هيئة التدريب العسكري	
جهاد عبد الكريم	48	بكالوريوس	الشرطة	وحدة حماية الأسرة	نائب مدير الإدارة	عقيد	ست سنوات	التحقيق، الأمن الداخلي، العمليات
باسل خريوش	49	ماجستير	الشرطة	وحدة حماية الأسرة	مدير الدائرة	مقدم	5 سنوات	شرطة نابلس
سامر حمد	43	بكالوريوس	الشرطة	وحدة الجرائم الإلكترونية		عقيد	20	المباحث
<p>○ هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟</p> <p>1- نعم 2. لا إذا كانت الإجابة نعم، كيف يكون التأثير؟</p>								
سونيا خليل عزاب	نعم إذا كان مستوى الذكاء العاطفي للمجرم عاليا يساعده على اختراق عقل الضحية بسهولة واستغلاله عاطفيا بشكل أكبر لوجود القدرة العالية لديه لمعرفة الوضع العاطفي للضحية، وفي حال كان مستوى الذكاء العاطفي للضحية عاليا يقلل ذلك من التعرض للابتزاز							
ديما يوسف عرب	العلاقة عكسية بين التعرض للابتزاز الإلكتروني ومستوى الذكاء العاطفي، كلما زاد الابتزاز، يكون مستوى الذكاء العاطفي قليل							
جهاد عبد الكريم	كلما تدنى مستوى الذكاء العاطفي لدى الشخص يؤدي إلى أن يكون عرضة للابتزاز الإلكتروني حيث إن الذكاء العاطفي المتدني يعكس شخصية ضعيفة.							
باسل خريوش	لا							
سامر حمد	نعم، يؤثر مستوى الذكاء العاطفي من حيث قدرة المبتز على تحليل مشاعر الضحية وفهم قدراته والمشاكل التي يعاني منها وهذا يكون مدخل لمعرفة كيفية الاحتيال عليها ثم الحصول على البيانات اللازمة							

○ برأيك/ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفي لدى الضحية؟

2- نعم لا

○ إذا كانت الإجابة نعم، كيف يكون التأثير؟

نعم				سونيا خليل عزاب
المتغير	يؤثر	لا يؤثر	كيف يؤثر	
الجنس	√		الأنثى اسهل للوقوع ضحية	
المستوى التعليمي			استهداف الشخص الذي يكون لديه مسمى وظيفي عالٍ يكون أكثر	
مكان السكن	√			
العمر		√	اخترق عقل الضحية يكون أسهل	
الوظيفة	√		من ناحية الحاق الضرر يكون عليه أكبر	
مستوى الدخل	√		إذا كان الهدف الحصول على مبلغ مالي	
الحالة الاجتماعية	√		تشكيل إفساد رابطة زوجية	
نعم				ديما يوسف عرب
المتغير	يؤثر	لا يؤثر	كيف يؤثر	
الجنس	√		على النساء	
المستوى التعليمي	√		يعطي قدر أكبر من الثقة والانفتاح	
مكان السكن	√		تؤثر من حيث التركيبة السكانية	
العمر	√		السنّ الكبير يعني النضج	
الوظيفة	√			
مستوى الدخل	√		لاستقلال المالي يرفع من التعرض للابتزاز	
الحالة الاجتماعية	√		يؤثر على النساء بشكل خاص للوضع الاقتصادي السيء	
لا				جهاد عبد الكريم
لا				باسل خريوش
نعم				سامر حمد
المتغير	يؤثر	لا يؤثر	كيف يؤثر	
الجنس	√		على النساء	
المستوى التعليمي	√		كلما كان المستوى التعليمي أعلى يؤثر أكثر	
مكان السكن		√		
العمر	√		الفئات العمرية الكبيرة	
الوظيفة	√		الوظيفة أعلى	
مستوى الدخل	√		الدخل المادي المرتفع	
الحالة الاجتماعية	√		الوضع الأسري	
ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟				
أكثر جرائم الابتزاز الإلكتروني تتمثل في ابتزاز الأنثى من خلال اختراق عقلها بداية واستغلالها عاطفياً والحصول على ثقتها وإبرام العهود المستقلة لها وبالتالي الحصول على صور ومقاطع فيديو لها ثم ابتزازها جنسياً أو مالياً وفي حالات ابتزاز كليهما، بالإضافة إلى ابتزاز الذكور أيضاً من خلال الحصول على مقاطع فيديو بإرادته مخلة بالأداب العامة.				سونيا خليل عزاب
الابتزاز عن طريق الصور والفيديوهات				ديما يوسف عرب
ابتزاز الفتيات من خلال الحصول على صور وفيديوهات لهن أو أي مادة أخرى تلحق بهن الضرر، وغالباً من يكون الهدف مالي				جهاد عبد الكريم
التشهير، التهديد، الاستغلال				باسل خريوش

سامر حمد	الابتزاز المالي، والجنسي
○ ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟	
سونيا خليل عزاب	وسائل التواصل الاجتماعي (فيس بوك، تويتر، واتس اب، انستغرام، سناب شات، ايمو...الخ)
ديما يوسف عرب	وسائل التواصل الاجتماعي
جهاد عبد الكريم	وسائل التواصل الاجتماعي
باسل خريوش	وسائل التواصل الاجتماعي
سامر حمد	وسائل التواصل الاجتماعي
○ ما أهم الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟	
سونيا خليل عزاب	قلّة الوعي لدى الضحية عند التواصل مع شخص عبر الإنترنت وبالتالي الوثوق به وإرسال الصور وفتح الكاميرا، ومقاطع الفيديو. 2. الفراغ وبالتالي استخدام هذه الوسائل بطريقة غير صحيحة 3. الحاجة إلى المال، فيلجأ البعض إلى استخدام الابتزاز للحصول على المال
ديما يوسف عرب	الضغط الأسري
جهاد عبد الكريم	قلّة الوعي وعدم النضج العاطفي.
باسل خريوش	العاطفة، الفقر، المشاكل الأسرية
سامر حمد	الإيقاع بالضحية من خلال حساب وهمي وممارسة الجنس من خلال الكاميرا عبر برامج الدردشة ولاحقا ابتزاز الضحية بالتسجيلات وأنه سيتم نشرها على الأقارب والأصحاب في حالة عدم الرضوخ للابتزاز
○ هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017)م على التقليل من نسبة جرائم الابتزاز الإلكتروني، كيف ذلك؟	
سونيا خليل عزاب	بشكل عام، نعم، لأنه معرفة الأشخاص بوجود القانون لهذا النوع من الجرائم يكون رادعا لهم لعدم القيام بها، ولكن آلة التعامل مع الجرائم الإلكترونية بشكل عام يتم التحفظ على هذه الجرائم وبالتالي عدم استكمالها قضائيا وهذا يعود لوضع المشتكية تحديدا وعدم رغبتها استكمال الشكوى، لم نلاحظ فرقا كبيرا من ناحية نقصان عدد القضايا من هذا النوع.
ديما يوسف عرب	نعم، لوجود مقومات يمكن استخدامها لردع المبتزين وحماية الضحية
جهاد عبد الكريم	القانون حديثة وتطبيقه يكون رادع للمبتز.
باسل خريوش	نعم، كونه رادع
سامر حمد	القانون لم يختبر حتى الآن
لماذا تمّ التعديل على قانون رقم (16) لعام (2017)م؟	
سونيا خليل عزاب	*بسبب الادعاء أو الاعتراض على آلية مجازاة مرتبكي الجريمة أي أن الأحكام المفروضة في القانون عالية ويجب تحقيقها
ديما يوسف عرب	لمواكبة التطورات الطارئة التي تحدث للمجتمع
جهاد عبد الكريم
باسل خريوش
سامر حمد	من باب التحديث وحسب الحاجة
○ ما هو القانون الحالي الذي يتم العمل به مع جرائم الابتزاز الإلكتروني ؟	
سونيا خليل عزاب	10 لسنة 2018
ديما يوسف عرب	10 لسنة 2018
جهاد عبد الكريم	قانون الجرائم الإلكترونية رقم 16 قانون العقوبات قانون الإجراءات الجزائية
باسل خريوش	...

سامر حمد	10 لسنة 2018
○ ما هي الإجراءات المتبعة من 'وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة' في التعامل مع جرائم الابتزاز الإلكتروني؟	
سونيا خليل عزاب	إجراءات إدارية قانونية حددها قانون الإجراءات الجزائية والقرار بقانون (10) من قانون الجرائم الجزائية
ديما يوسف عرب	سماع الشكوى، التحقيق في الواقعة، دراسة الاحتياجات والنتائج، وحدة الجرائم الإلكترونية
جهاد عبد الكريم	لدى إدارة حماية الأسرة يتم استقبال الشكاوي وضبط المواد المستخدمة في الابتزاز وتحويلها لوحدة الجرائم الإلكترونية لجمع الاستدلالات، ومن ثم تحويل القضية للوحدة العامة المختصة ليتم الإجراء القانوني بحقه
باسل خريوش	استقبال الضحية وسماعها، تدوين الإفادة، إحالة الملف إلى جهات الاختصاص في وحدة الجرائم الإلكترونية، تحويل الملف إلى الوحدة العامة والقضاء
سامر حمد	إدارية ترتبط بالقانون والإجراءات الجزائية وقفية وترتبط بعمل الأدوات المستخدمة ويتم الفحص من خلال الأدوات.
○ ما هي الإجراءات المتبعة من 'وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة' لحماية ضحايا جرائم الابتزاز الإلكتروني؟	
سونيا خليل عزاب	تخصص وحدة حماية الأسرة
ديما يوسف عرب	حماية المعلومات والتعامل بسرية
جهاد عبد الكريم	تعمل وحدة حماية الأسرة بعد وحدة الجرائم الإلكترونية لحماية الضحايا إذا كان هناك تقدير يشير بوجود خطر عليهم سواء من المشتبه به أو من الأسر وذلك من خلال إيداع الضحية في مراكز الإيواء وأجراء التدخلات الاجتماعية والنفسية المناسبة
باسل خريوش	
سامر حمد	الحماية هي من صلاحيات وحدة حماية الأسرة
○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟	
سونيا خليل عزاب	*الآثار النفسية قد تتأثر الضحية وتحديدا الفتاة نفسيا وذلك بالشعور بفقدان الثقة بالنفس والقدرة على مواجهة المجتمع كالسابق، الآثار المادية
ديما يوسف عرب	أضرار اقتصادية، مشاكل في الحياة الزوجية، الخطورة على حياة الضحية
جهاد عبد الكريم	وقوع الضحية في دائرة الخطر على حياتها وما يترتب عليها من آثار نفسية واجتماعية
باسل خريوش	آثار نفسية، مشاكل أسرية، وجود خطوة على حياة الضحية، آثار اقتصادية
سامر حمد	تؤثر على الأسرة وتسهم في التفكك الأسري، قد تؤدي بحياة الضحية في بعض الحالات
ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟	
سونيا خليل عزاب	نظرة المجتمع للوسائل، وسائل التواصل الاجتماعي، وذلك عن قراءة أو ملاحظة وجود عدد كبير من هذا النوع من الجرائم ويتم خلال استخدام هذه الوسائل وبالتالي فقدان الثقة.
ديما يوسف عرب	التفكك المجتمعي، عدم الإحساس بالمسؤولية، عدم الثقة بالتعاملات الاقتصادية مع الآخرين
جهاد عبد الكريم	ازدياد الجريمة وخاصة على الفتيات، خلل في النظام الاجتماعي ناتج عن نقص الثقة، ازدياد هذا النوع من الجرائم يؤدي إلى تكوين ظاهرة وثقافة خطيرة خاصة لدى فئة الشباب والمراهقين يصعب السيطرة عليها في المستقبل.
باسل خريوش	تفكك أسري، عزلة اجتماعية
سامر حمد	تؤثر على الأسرة وتساهم في التفكك الأسري وقد تؤدي بحياة الضحية، فقدان الثقة، مشاكل اجتماعية وتفكك اسري
○ ما هي الصعوبات التي تحد من عمل 'وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة'، من وجهة نظرك/ي؟	
سونيا خليل عزاب	استخدام الشرائح الإسرائيلية لارتكاب هذه الجرائم وبشكل عام يصعب ملاحقة المرتكبين

*الانقسام الفلسطيني أيضا يشكل صعوبة لملاحقة المرتكبين إذا كان من قطاع غزة	
*زيادة استخدام الإنترنت من خلال شرائح G 3	
الخوف من فكرة التحقيق والادعاء أمام الوحدة.	ديما يوسف عرب
تردد بعض الحالات في اللجوء لإدارة حماية الأسرة لتقديم الشكوى. نقص الرتب وخاصة من يملكون الخبرة في التعامل في مجال الوسائل الإلكترونية والقانونية.	جهاد عبد الكريم
الموقع الجغرافي بشكل عام يؤدي إلى عدم القدرة على السيطرة	باسل خربوش
كونها جريمة جديدة تحتاج إلى دقة وخبرة في التعامل معها، كما أنّ استخدام الشرائح الإسرائيلية.	سامر حمد
• من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز الإلكتروني، الرجاء ترتيبها حسب الأولوية؟	
8 رقم موحد للتبليغ عن الجرائم الإلكترونية. 4 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات. 5 الحرص على تقديم الجاني للمحاكمة. 1 حملات توعية مجتمعية. 2 مؤتمرات ومحاضرات. 9 تفعيل دور الرقابة المجتمعية. 3 اكتساب ثقة المواطنين. 6 نشر قصص نجاح للتأكيد على أهمية التدخل المهني. 7 دعم الضحية وحمايته	سونيا خليل عزاب
1 رقم موحد للتبليغ عن الجرائم الإلكترونية. 5 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات. 6 الحرص على تقديم الجاني للمحاكمة. 2 حملات توعية مجتمعية. 7 مؤتمرات ومحاضرات. 3 تفعيل دور الرقابة المجتمعية. 4 اكتساب ثقة المواطنين. 9 نشر قصص نجاح للتأكيد على أهمية التدخل المهني. 8 دعم الضحية وحمايته.	ديما يوسف عرب
2 رقم موحد للتبليغ عن الجرائم الإلكترونية. 3 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات. 4 الحرص على تقديم الجاني للمحاكمة. 7 حملات توعية مجتمعية. 8 مؤتمرات ومحاضرات. 6 تفعيل دور الرقابة المجتمعية. 1 اكتساب ثقة المواطنين. 9 نشر قصص نجاح للتأكيد على أهمية التدخل المهني. 5 دعم الضحية وحمايته.	جهاد عبد الكريم
4 رقم موحد للتبليغ عن الجرائم الإلكترونية. 1 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات. 9 الحرص على تقديم الجاني للمحاكمة. 2 حملات توعية مجتمعية.	باسل خربوش

<p>3 مؤتمرات ومحاضرات.</p> <p>6 تفعيل دور الرقابة المجتمعية.</p> <p>5 اكتساب ثقة المواطنين.</p> <p>8 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.</p> <p>7 دعم الضحية وحمايته</p>	
<p>7 رقم موحد للتبليغ عن الجرائم الإلكترونية.</p> <p>3 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.</p> <p>3 الحرص على تقديم الجاني للمحاكمة.</p> <p>2 حملات توعية مجتمعية.</p> <p>2 مؤتمرات ومحاضرات.</p> <p>6 تفعيل دور الرقابة المجتمعية.</p> <p>1 اكتساب ثقة المواطنين.</p> <p>5 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.</p> <p>4 دعم الضحية وحمايته.</p>	<p>سامر حمد</p>

مناقشة النتائج والتوصيات

في هذا الفصل سيتم عرض لكافة نتائج الدراسة في ضوء الإطار النظري والدراسات السابقة ذات العلاقة والنظريات المفسرة للإجابة عن الأسئلة التي طرحت حيث تمثل مشكلة الدراسة، بعد أن تمت عملية جمع البيانات اللازمة بواسطة أدوات الدراسة (الاستبانة، والمقابلة)، التي من خلالها تمّ التوصل إلى عدد من النتائج وعلى ضوءها تمّ وضع عدد من التوصيات.

1.5 مناقشة نتائج أسئلة وفرضيات الاستبانة:

مناقشة نتائج السؤال الرئيس للدراسة وهو:

ما علاقة الذكاء العاطفي بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية؟

وسيتم الإجابة عليه من خلال سؤالي الدراسة الأول والثاني:

مناقشة النتائج المتعلقة بالسؤال الأول:

ما مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني؟

من خلال إجراء التحليل الإحصائي تبين بأن مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني جاء بدرجة متوسطة حسب استجاباتهم لفقرات الاستبانة التي بيّنها الجدول البياني رقم (1.4)، حيث بلغ المتوسط الحسابي للدرجة الكلية (3.39) وانحراف معياري (0.411)، حيث أظهرت النتائج أنّ الفقرة رقم (16) التي نصّها " أتعامل مع الآخرين باحترام متبادل " حصلت على أعلى متوسط حسابي (4.34)، يليها الفقرة رقم (26) التي نصّها " أحزن لحزن الناس " بمتوسط حسابي (4.29). وحصلت الفقرة رقم (33) التي نصّها " أشعر بان الواقع (زائف، وخداع) " على أقلّ متوسط حسابي (2.34)، يليها الفقرة رقم (41) التي نصّها " تحاصرني الهموم من كلّ اتجاه " بمتوسط

حسابي (2.53)، إذ تبين من النتائج أن تدني المستوى الذكاء العاطفي لدى الفرد قد يؤدي إلى زيادة احتمالية تعرضه لجريمة الابتزاز الإلكتروني، حيث إنّ الذكاء العاطفي يتكون من عدة مكونات، ذلك وفق وجهة نظر "ماير وسالوفي" إذ تتمثل في: (الوعي بالذات: التي تعني وعي الفرد بمشاعره وانفعالاته وعواطفه وأفكاره المرتبطة بها، وكبت الانفعالات: التي تعني قدرة الفرد على التحكم في مشاعره وضبطها، والاستعداد الرئيسي: تعني الطاقة الداخلية التي تؤثر بشدة في القدرات الإيجابية والسلبية وإعاقتها، والفنون الاجتماعية: أساس العلاقات مع الآخرين هو إدارة الانفعالات، حيث يتطلب التعامل مع مشاعر الآخرين ارتفاع مستوى مهارتين هما: إدارة الذات، والتعاطف مع الآخرين، إنّ القصور في إدارة الذات والتعاطف مع الآخرين يؤدي إلى تعرض الفرد إلى المشكلات المختلفة والمتنوعة، والتعاطف: تُعدّ القدرة على فهم مشاعر الآخرين وقراءتها من خلال صوتهم أو تعبيرات وجوههم، فلا يقتصر ذلك على الرسائل المباشرة التي يوجهوها لغيرهم).

لذا كلما كان الفرد على وعي بعواطفه وانفعالاته، كان أكثر مهارة على قراءة مشاعر الآخرين، فالفضل في إدراك مشاعر الآخرين هو نقطة عجز أساسية في الذكاء العاطفي، حيث توضح استجابات عينة البحث نحو فقرات الاستبانة التي بيّنها الجدول البياني رقم (1.4) أن هناك تفاوتاً في مستوى كلّ مكون من مكونات الذكاء العاطفي، حيث ينعكس ذلك على شخصيّة الضحية التي قد تكون غير قادرة على الموازنة بين ذاتها والآخرين وتوفير الفهم الكافي للانفعالات والتحكم فيها، ممّا يؤدي إلى وجود ثغرة يستغلها الجاني للوصول لضحيته حتى يقوم بابتزازها، ممّا يعني أن الجاني يتمتع بمستوى عالٍ من الذكاء العاطفي يساعده على اكتشاف ضحيته بسهولة واستغلالها لتحقيق غايته.

كما يمكن القول: إنّ الأفراد الأذكاء عاطفياً يتمتعون بعدة سمات تميزهم عن الأفراد الذين لا يتمتعون بذكاء عاطفي، إذ لا يشترط كلّ الصفات والمهارات والقدرات السابقة أن تتواجد بالفرد بسبب الفروق الفردية والاختلافات التي تميّز الأفراد عن بعضهم بعضاً، بالإضافة إلى تأثير المتغيرات الديموغرافية المختلفة على مستوى الذكاء العاطفي لدى الفرد منها (العمر، والجنس، ومكان السكن، والتعليم)، جميع المؤثرات السابقة تؤثر على مستوى الذكاء العاطفي لدى الفرد بالإضافة إلى استعداد الشخصيّة ودافعيته لرفع مستوى ذكائه العاطفي، هذا ينطبق على الجناة (المبتزين) من الممكن أن يكون الجناة متمتعين بذكاء عاطفي مرتفع فيكون قادراً على معرفة انفعالاته ومشاعره وإدارتها وفهم الضحية، خاصة الضحايا الذين يقعون في فخ جرائم الابتزاز الإلكتروني التي تظهر ببساطة الفرد ذي الذكاء

العاطفي المنخفض عند عدم قدرته الرفض أو التعامل مع التهديدات التي يقوم بها الجاني نحوه، أو قد يكون غير قادر على وضع حدود بعلاقته مع الجاني، فيشعر بالاستياء دون القدرة على إظهار هذا الشعور، الأمر الذي يجعله يخضع لما يطلبه الجاني حتى ولو كان أمراً غير أخلاقي.

تتفق هذه النتيجة مع دراسة (Catalan, and Zych, and Ruiz, and Llorent, 2017)، بعنوان "الضحية من خلال الجرائم الإلكترونية (البلطجة والتسلط الإلكتروني): الذكاء العاطفي، وشدة الإيذاء واستخدام التكنولوجيا في أنواع مختلفة من الضحايا"، التي أشارت إلى أنّ الضحايا الذين يقعون ضحايا في الحياة الواقعية هم أكثر عرضة لأن يكونوا ضحايا للجرائم الإلكترونية، وأنّ الذكاء العاطفي قد يحمي الأفراد من الوقوع كضحايا بالعالم الافتراضي والواقعي.

يمكن القول: إنّ هذه النتيجة تعود إلى أنّ مستوى الذكاء العاطفي المتوسط وتفاوت مكوناته لدى الضحايا يسهم في زيادة تعرضهم للابتزاز الإلكتروني من قبل الجناة، إضافة إلى أنّ أغلب الجناة الذين يستخدمون الابتزاز الإلكتروني تكون مستويات الذكاء العاطفي لديهم مرتفعة، وهذا يساعدهم في تخطي أي عواقب يمكن أن تواجههم في علاقتهم مع الضحية للحصول على غايتهم منها، كذلك يسهم ارتفاع رغبة الضحية بسد الفراغ العاطفي لديها في سهولة قيام المبتزين للقيام بفعلتهم، هذا ما تتفق معه دراسة (Megreya, 2014)، بعنوان "الذكاء العاطفي والسلوك الجنائي". حيث أشارت هذه الدراسة أنّ الجناة الذين يقومون بعدوان مباشر انخفض لديهم مستوى الذكاء العاطفي، بينما الجناة الذين يقومون بالقيام بارتكاب جريمتهم بشكل غير مباشر يتمتعون بمستوى ذكاء عاطفي أكبر، وبالإمكان تخفيض السلوك الإجرامي من خلال تحسين قدرات الذكاء العاطفي مثل: إدارة الغضب والانفعالات، وغير الجناة يتمتعون بمستوى ذكاء عاطفي أكبر من الجناة في الدراسة لأنهم قادرين على فهم ذاتهم وفهم الآخرين والتحكم في ذاتهم وانفعالاتهم، إضافة إلى كون هذه النتيجة تتفق مع نتيجة السؤال الأول في المقابلات الذي ينص على "هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟"، حيث أشارت نتائجها بأن مستوى الذكاء العاطفي يؤثر بشكل كبير على زيادة ممارسة جرائم الابتزاز الإلكتروني، ذلك بسبب اقتران ارتفاع مستوى الذكاء العاطفي للجاني بقدرته على فهم مشاعره وانفعالات الضحية، خاصة فيما يتعلق في الجانب الأسري والاجتماعي للضحية ليستغل أي ضعف متمثل (خلافات أسرية، أو تفكك أسري، أو إهمال العلاقات، أو عزلة اجتماعية، أو عنف، أو إدمان، .. الخ)، لذا يقوم لاحقاً باستغلال العوامل والظروف المحيطة

بالضحية بالإضافة إلى استغلال عدم قدرة الضحية على فهم مشاعر وانفعالات الآخرين وعدم القدرة على إدارة المشكلات وإيجاد الحلول، فيجعل كل ما سبق مقومات في اختيار الضحية المناسبة لممارسة فعلته المتمثلة بالابتزاز والاستغلال ليصل إلى هدفه.

في حين تختلف هذه النتيجة مع دراسة (Ojedokun, and Idemudia, 2013)، بعنوان " الدور المعتدل للذكاء العاطفي بين العوامل الشخصية والجرائم الإلكترونية(البلطجة الإلكترونية) في العديد من مجتمعات الطلاب"، التي أشارت إلى أن من يقوم بارتكاب الجرائم الإلكترونية غير المنظمة يتميز بتدني مستوى الذكاء العاطفي، وتتفق مع نتائج الدراسة في أن مرتكبي الجرائم لديهم ارتفاع في مستويات الأمراض الذهانية والعصبية.

مما سبق يمكن تفسير هذه النتيجة في ضوء نظرية "مايروسالوفي" ، التي ترى بأن الشخص الذكي عاطفياً أفضل من غيره في التعرف على الانفعالات سواء كانت انفعالات الشخص ذاته أو انفعالات الآخرين، ولديه القدرة على التعبير العاطفي بصورة واضحة ودقيقة، وأن هناك فروقاً فردية ما بين الأفراد من ناحية مستوى الذكاء العاطفي لديهم وفق لمكوناته (مقدراته)، لذا نلاحظ الاختلاف بقدرة الفرد بالموازنة بين عواطفه وردود أفعاله وبين الاستجابة وفهم الآخرين، فنجد الأفراد الذين لا يستطيعون تحقيق هذه المعادلة ينجرون وراء عواطفهم، لأنه لا يكون لديهم القدرة على فهم وإدراك عواطفهم، واستثمارها للقيام بأنشطة إدراكية مثل حل مشكلاتهم، بالتالي لا يديرون عواطفهم، مما يجعلهم فرصة مناسبة يسعى الجناة لإيقاعهم في فخ جرائم الابتزاز الإلكتروني التي تلعب على وتر العاطفة والفراغ لدى الضحية في أغلب الأحيان.

وتتفق هذه النتيجة مع دراسة (الخليوي، 2014) بعنوان " دور مواقع التواصل الاجتماعي في زيادة جريمة الابتزاز ضد المرأة من وجهة نظر طالبات الجامعات السعودية "، حيث أشارت الدراسة إلى أن مواقع التواصل الاجتماعي سهلت للمبتز تهديد الضحية، وسهولة التواصل والتعارف وإقامة علاقات محرمة بين المبتز والفتاة، ضعف الوازع الديني لدى المبتز، ضعف العقوبات الرادعة لجرائم الابتزاز الإلكتروني، ضعف الرقابة الأسرية على الأبناء، العادات والتقاليد قد تخضع الفتاة للاستمرار في الخضوع للمبتز، التطور التقني ساعد في سهولة اتصال الشاب بالفتاة، لذلك على الأسرة تقوية الوازع

الديني لدى أبنائها احتواء مشاكل الفتاة وتوعيتها بعواقب العلاقات العاطفية وتفعيل دور الحوار فيما بينها وبين أبنائها.

مناقشة نتائج السؤال الثاني:

ما واقع ممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية؟

وسيتم الاجابة عليه من خلال مناقشة الاسئلة الفرعية الآتية:

مناقشة نتائج السؤال الفرعي الأول:

ما الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني؟

أشارت النتائج الموضحة في الجدول البياني رقم (3.4) وفق استجابات المبحوثين لفقرات الاستبانة للمحور الثاني "الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني" ، بلغ المتوسط الحسابي للدرجة الكلية (4.02) وانحراف معياري (0.676). حيث حصلت الفقرة رقم (1) التي نصّها "العلاقات العاطفية " على أعلى متوسط حسابي (4.34)، يليها الفقرة رقم (15) التي نصّها "إرسال المبتز معلومات خاصة به لكسب ثقة الضحية" بمتوسط حسابي (4.33). وحصلت الفقرة رقم (13) التي نصّها "استخدام المواقع الإباحية كوسيلة لأغراء الضحية " على أقلّ متوسط حسابي (3.66)، يليها الفقرة "الدخول إلى حساب الضحية من خلال الهكر" والفقرة رقم (10) التي نصّها "استغلال المبتز غياب الرقابة على مواقع التواصل الاجتماعي" بمتوسط حسابي (3.74).

تشير النتائج السابقة إلى أنّ الوسائل المستخدمة للابتزاز الإلكتروني جاءت بدرجة مرتفعة، هذا يتفق مع (دراسة النصر، 2017)، بعنوان "التحقيق في جرمي التحرش والابتزاز عبر الشبكات الإلكترونية - دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية"، التي أشارت إلى أنّ مدى انتشار جريمة الابتزاز عبر الشبكات الإلكترونية من وجهة نظر المحقق في هيئة التحقيق والادعاء العام بالمنطقة الشرقية كان مرتفعاً.

ويمكن تفسير هذه النتيجة بأنّ الجاني في أغلب الأحيان يلجأ لاستخدام العلاقات العاطفية من أجل الوصول إلى الضحية، ذلك حسب مستوى الذكاء العاطفي للضحية، حيث يصل في بعض الأحيان

إلى الوعد بالزواج، وهنا يمكن للضحية أن تستجيب بإرسال الصور أو الفيديوهات المختلفة، فيصبح الجاني مسيطرا عاطفياً على الضحية، وإخضاعها له بحجة العلاقة فيما بينهم، وذلك للوصول إلى غايته من خلال التهديد والابتزاز بإنهاء هذه العلاقة إن لم تستجب الضحية له، فيستهدف الجاني الأفراد (الضحايا) الذين يفتقرون لوجود الجنس الآخر في حياتهم لإشباع رغباتهم العاطفية وفي بعض الأحيان رغباتهم الجنسية، حيث إن هذه المرحلة مهمة في حياة الأفراد ويمكن من خلالها السيطرة على الانفعالات الخاصة بالضحية، كما أنّ الحاجة إلى وجود علاقات اجتماعية عالية أسوة بالزملاء أسهم في نشر ثقافة التعارف من خلال مواقع التواصل الاجتماعي، التي يكون في اللقاء من خلال الإنترنت سواء باستخدام الحاسوب أو باستخدام الهاتف، وما ساعد على انتشار هذه الطريقة، هي وجود الثقافة الذكورية التي تمنع وجود أي علاقات صداقة أو زمالة بين الذكور والإناث في المرحلة الجامعية، الأمر الذي يشجع الطرفين على اللقاء من خلال مواقع التواصل الاجتماعي والبوح بكافة المشاعر التي يحملها الطرف إلى الآخر، وفي هذه الحالة تنتج علاقات مختلفة تصل في بعض الأحيان إلى الثقة المطلقة، وعادة ما يبحث المبتز في علاقة عامة يهدف منها الحصول على المال أو الجنس، وهي الحاجات التي يفتقرها سواء أكان أعزب أم لا يعمل، أو كان متزوجاً لا يحصل على الحاجات الخاصة بالجنس من الشريك، وينتج عن هذه العلاقات مع الوقت منظومة تبادلية من المعلومات المشتركة اليومية، التي يستغلها الجاني ويستخدمها من أجل ما يسعى إليه وهو ابتزاز الضحية والحصول على ما يريد، وقد تكون المعلومات الخاصة به في أغلب الأحيان وهمية ويتم استخدامها من أجل كسب ثقة الضحية وجعلها بالمقابل ترسل معلومات خاصة بها (صور، أو فيديو، أو الاسم... الخ) من ثم استخدامها ضد الضحية في حالة المعارضة أو عدم الاستجابة له، ذلك وفقاً للغاية التي يريدها قد تكون (مادية، أو جنسية... الخ) مستخدماً نكاهه العاطفي وقدرته على الإقناع.

وتتفق هذه النتيجة مع نتيجة السؤال الثالث في المقابلة الذي ينص على " ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟"، حيث أشارت النتائج إلى أنّ أهم الوسائل المستخدمة للإيقاع بالضحية تتمثل في جمع المعلومات والبيانات الخاصة بالضحية سواء من خلال العلاقات العاطفية واكتساب ثقتها من خلال إرسال معلومات عنه، إضافة إلى اختراق حسابات الضحية دون معرفتها للحصول على معلومات شخصية، أو صور، أو فيديو أو أي شيء يتعلق بها ويمكن استغلاله لارتكاب جريمة الابتزاز الإلكتروني.

وهذا ما تتفق معه دراسة (Hampson,2012)، بعنوان " دور الذكاء العاطفي في النشاط الإجرامي للشباب المشاركين في خدمة ليدز للشباب المخالفة"، حيث أشارت هذه الدراسة إلى هناك ضرورة لدراسة الذكاء العاطفي في الجرائم فهو يتيح فرصة للتعاطف مع الضحايا، ويجب أن يكون هناك فرصة للشباب المشتركين في خدمة ليدز لتطوير الذكاء العاطفي لديهم لكي يتمكنوا من تقدير مشاعر الآخرين، وفهم عواطفهم.

مناقشة نتائج السؤال الفرعي الثاني:

ما الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني؟

أشارت النتائج الموضحة في الجدول البياني رقم (4.4) وفق استجابات المبحوثين لفقرات الاستبانة (أهم الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني) إذ بلغ المتوسط الحسابي للدرجة الكلية (3.90) وانحراف معياري (0.593)، وهذا يدل على أن الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني جاءت بدرجة عالية، كما وتشير النتائج في الجدول رقم (3.4) أن (16) فقرة جاءت بدرجة عالية و (5) فقرات جاءت بدرجة متوسطة. وحصلت الفقرة رقم (13) التي نصّها "الاختلاط بأصدقاء السوء" على أعلى متوسط حسابي (4.49)، يليها الفقرة رقم (8) التي نصّها "ضعف الوازع الديني" بمتوسط حسابي (4.41)، وحصلت الفقرة رقم (19) التي نصّها "عدم الثقة بالقضاء" والفقرة رقم (11) والتي نصّها "استفزاز الضحية للمبتز" على متوسط حسابي (3.89) والفقرة رقم (18) التي نصّها "عدم الثقة بالوحدة" على أقلّ متوسط حسابي (3.48)، يليها الفقرة رقم (4) التي نصّها "ضعف تنفيذ القوانين الخاصة بالجرائم الإلكترونية" بمتوسط حسابي (3.53).

يمكن تفسير ذلك من خلال نظرية التقليد التي لم يتم توضيحها خلال الإطار النظري لكثرة النظريات المفسرة لجريمة الابتزاز الإلكتروني، ذلك لأنّ هذه الجريمة مكتملة الأركان مثل باقي الجرائم ويتم تفسيرها على هذا الأساس، لذا يمكن تفسير جريمة الابتزاز الإلكتروني بأنها قد تنتج من خلال نمط سلوكي لفرد يمثل قدوه لآخرين فيقومون بتقليده، لكن من الممكن أن يمثل القدوة أحد رفاق السوء إذ يؤثر في طبيعة التفكير لدى الضحية خاصة الشباب، ليلجأ البعض منهم لتقليد بعضهم البعض دون التفكير بعواقب الأمور حيث يمثل هذا تدنيا في مستوى الذكاء العاطفي لديه، ممّا يوقعه في فخ الجرائم الإلكترونية (الابتزاز الإلكتروني) فقد لا يكون الضحية مقتنعا بإقامة علاقات عاطفية مع الجنس

الآخر، لكن في ظل وجود أصدقاء يقومون بذلك، ويعملون على خلق قنوات لدى أصدقائهم بضرورة تجريب مثل هذه العلاقات، من باب التباهي والتحدي الذي يكون عادة بين الرفاق، وبأن هذه العلاقات مجرد تسالي يومية وتنتهي في مرحلة زمنية معينة، يؤدي في النهاية إلى قبولها، ولعدم توفر الخبرة الكافية عند التعامل مع الطرف الآخر قد لا يراعي الحدود في العلاقة نتيجة ضعف الوازع الديني، ليصل به الأمر إلى علاقة غير مسيطر عليها، وقد تؤدي إلى وقوعه في فخ جرائم الابتزاز الإلكتروني، مما يقوده للخضوع للطرف المبتز نتيجة تعلقه به للمحافظة على هذه العلاقة، خاصة الضحايا الذين يعانون من الفراغ العاطفي والتوتر الناجم عن التفكك الأسري.

وهذه النتيجة تتفق مع دراسة (الخليوي، 2014)، بعنوان " دور مواقع التواصل الاجتماعي في زيادة جريمة الابتزاز ضد المرأة من وجهة نظر طالبات الجامعات السعودية "، التي أشارت إلى أن مواقع التواصل الاجتماعي سهلت للمبتز تهديد الضحية، سهولة التواصل والتعارف وإقامة علاقات محرمة بين المبتز والفتاة، وضعف الوازع الديني لدى المبتز، وضعف العقوبات الرادعة لجرائم الابتزاز الإلكتروني، وضعف الرقابة الأسرية على الأبناء، والعادات والتقاليد قد تخضع الفتاة للاستمرار في الخضوع للمبتز.

كما تشير النتائج إلى أن هناك مستوى منخفض لدى الفتيات في معرفة أنواع وأشكال جرائم الابتزاز الإلكتروني، ووجود مستوى مرتفع من الثقة في الأفراد الذين يتم الحوار معهم على مواقع التواصل الاجتماعي باعتبارهم أفرادا ذوي مستوى تعليمي مرتفع كما يعرفون عن أنفسهم، أو لديهم مستوى عمل ودخل جيد، ويسهم في رفع مستوى ثقة الضحية بالطرف الآخر وهو ما أشارت إليه دراسة (بنت حجاب، 2016)، بعنوان " تصور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الابتزاز "، التي أشارت إلى وجود ضعف لدى الفتيات في جانب معرفة أنواع جرائم الابتزاز الإلكتروني وأشكالها كافة، مما يعني وجود حاجة لتنمية الوعي الوقائي بجرائم ابتزاز الفتيات.

وكما تتفق هذه النتيجة مع نظرية التعلق التي تفيد بأن الفرد بحاجة إلى إن يبني علاقات إنسانية ودية وثيقة خاصة العاطفية منها، ويزداد هذا الشعور عند الإحساس بالخطر والتهديد أو في المواقف الضاغطة مثل حالات التفكك الأسري، أو الضغوطات الاجتماعية، مثل ضغوط الأقران أو الضغوطات المالية، مما يرفع مستوى التوتر لديه ويكون بحاجة إلى سد حاجته العاطفية من خلال

التعلق بفرد معين دون الأخذ بعين الاعتبار المخاطر والخسائر التي قد تلحق به من هذه العلاقة، ذلك محاولة منهم للشعور بالأمان وخفض مستوى التوتر لديهم من خلال التعلق بفرد ما، لكن قد يتم الاختيار من خلال الاستخدام المتهور لمواقع التواصل الاجتماعي والتعرف على غرباء دون التفكير بالعواقب للحصول على علاقات يطمح من خلالها التخلص من التوتر والحصول على الأمان، وبهذا يكون على استعداد للقيام بما يمليه عليه الطرف الآخر دون الأخذ بعين الاعتبار أنّ هذه العلاقة قد تصل للاستغلال، نتيجة تدني مستوى الذكاء العاطفيّ لديه وعدم قدرته على حلّ مشاكله وإيجاد الحلول المناسبة، وعدم قدرته على التخلص من الخوف والتوتر لديه بنفسه وترجمة وفهم مشاعره ومشاعر الطرف الآخر، ممّا يجعله ضحية مناسبة لارتكاب جريمة الابتزاز الإلكترونيّ وحصول الجاني على مبتغاه دون تعب أو مجهود.

كما أشارت النتائج إلى أنّ استفزاز الضحية للجاني جاء بدرجة عالية، وهذا يتوافق مع نظرية العالم "مارفن وولفغانك" بعنوان تهور المجني عليه، حيث يعمل المجني عليه لاستفزاز الضحية وتحديه ممّا يساعد في قيام الجاني بمحاولة إثبات قدرته على التحدي، خاصة بعد قيام الضحية بقطع العلاقة معه أو رفض طلباته المختلفة، فيقوم الجاني بإيقاع الضحية في فخ الإبتزاز، كما وتتفق النتائج مع دراسة (الشمري، 2011) بعنوان "دور الضحية في حصول الفعل الإجراميّ من منظور طلاب الجامعة"، التي وضحت أن دور الضحية الاستفزازي للمجرم جاء بالمرتبة الأولى، ويمكن تفسير ذلك بأنّ الضحية عادة ما تكون السبب في حصول الجريمة، وذلك من خلال إجبار الجاني على القيام بعملية الإبتزاز، إذ عندما تقوم الضحية بقطع الصلة فجأة بالجاني بعد علاقة عاطفية لمدة زمنية طويلة، أو بعد علاقة صداقة طويلة الأمد، يحصل حينها رد فعل عكسي لدى الجاني، الذي بدوره يبدأ بتهديد الضحية، أو من خلال طريقة حياة وأسلوب الضحية، حيث هناك الكثير من الأفراد يحاولون فرض أنفسهم على الآخرين، فيعتمد الجاني أسلوب ابتزاز الضحية من أجل التخلص منها، إضافة إلى ذلك تتفق نظرية تهور المجني عليه مع نظرية ديسك التي تنصّ على أنّ نمط شخصية الفرد يؤثر بشكل كبير على أسلوب حياته وطريقة تعامله مع الآخرين، فنمط الشخصية المتهور والمندفع يكون في ذات الوقت متهورا في أفعاله وأسلوب حياته ممّا يزيد فرص وقوعه ضحية لجرائم الابتزاز الإلكترونيّ.

وتتفق هذه النتيجة مع نتيجة السؤال الرابع في المقابلات الذي ينصّ على " ما الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟"، إذ تشير النتائج إلى أنّ عدم استغلال وقت الفراغ بالشكل الصحيح ومرافقة رفاق سوء والفراغ العاطفي قد يسهمون في سهولة وقوعهم كضحايا للابتزاز الإلكتروني، إضافة إلى الثقة المطلقة التي يوليها الأفراد الذين يستخدمون هذه المواقع في التعارف والتسلية.

مناقشة نتائج السؤال الفرعي الثالث:

ما هي الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع ضحايا جرائم الابتزاز الإلكتروني؟.

للإجابة عن هذا السؤال تمّ حساب المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عيّنة الدراسة على فقرات الاستبانة التي تعبر عن الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة" في التعامل مع جرائم الابتزاز الإلكتروني، تشير النتائج في الجدول البياني رقم (5.4) إلى أنّ استجابات أفراد عيّنة الدراسة على الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز الإلكتروني أنّ المتوسط الحسابي للدرجة الكلية (4.12) وانحراف معياري (0.409) وهذا يدل على أن الإجراءات المتبعة من " وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز الإلكتروني جاءت بدرجة عالية.

كما وتشير النتائج في الجدول رقم (4.4) أن (15) فقرة جاءت بدرجة عالية وفقرة واحدة جاءت بدرجة متوسطة. وحصلت الفقرة رقم (15) التي نصّها "جميع إجراءاتها تتمّ بسرية تامة، ذلك للحفاظ على سمعة الضحية " على أعلى متوسط حسابي (4.47)، يليها الفقرة رقم (1) التي نصّها " إتباع قانون الجرائم الإلكترونية في فرض العقوبة المناسبة على المبتز " بمتوسط حسابي (4.40). وحصلت الفقرة رقم (7) التي نصّها "اللجوء إلى الجهات العشائرية لحل جريمة الابتزاز الإلكتروني بطرق ودية"

على أقلّ متوسط حسابي (3.47)، يليها الفقرة رقم (3) التي نصّها "استخدام الضحية كأداة للمساعدة في القبض على المبتز" بمتوسط حسابي (3.71).

من النتائج السابقة يتضح أنّ وحدة الجرائم الإلكترونية ووحدة حماية الأسرة تتلقى شكاوى فيما يخص عمليات الابتزاز، هذا يعود إلى توجه الضحية إلى وحدة الجرائم الإلكترونية، وقد تكون النسبة بشكل عام متدنية إلا أنّها موجودة، كما تعمل وحدة الجرائم الإلكترونية بشكل سريّ فيما تحصل عليه من معلومات، وتقوم باتباع القانون في التحقيق وفرض العقوبة على المبتز، وعادة لا يتم استخدام الضحية كأداة من أجل الضغط على المبتز للحصول على المعلومات منه، وحسب نتائج المقابلات، فقد تبين أنّ الإجراءات عادة ما تكون إدارية مرتبط بالقانون، وإجراءات فنية مرتبطة بعمل الأدوات المستخدمة داخل الوحدة، وسماع الشكاوي والتحقيق في الواقعة وتحديد الاحتياجات والنتائج حسب الاختصاص، إنّ حصول هذه النتيجة على أعلى متوسط حسابي منطقي فلولا السرية في التعامل مع هذه القضايا لما كان هناك شكاوي من الضحايا، إنّ طمأننة الضحايا بأنّ أية شكوى تُقدم بمعلوماتها كاملة تُعامل بسرية تدفعهم لتقديم الشكاوى من أجل الحصول على حقهم وحلّ المشكلة التي تواجههم.

إنّ وحدة الجرائم الإلكترونية ووحدة حماية الأسرة عادة ما تتابعان البلاغات المتعلقة بالجرائم الإلكترونية بعد وصول الشكاوى من الضحية، من خلال إجراءات لمتابعة المبتز والقبض عليه، من خلال المعلومات التي وفرها الضحية حول عنوانه الإلكتروني وكل ما يخص ذلك، حيث يتمّ متابعته من أجل منع تورط ضحايا آخرين، ومن أجل التحقيق في الأسباب التي دفعت المبتز للقيام بذلك ثمّ معاقبته، لذلك من المهم أن يتم إبلاغ الوحدة العامة من قبل الضحايا عند بداية الابتزاز الإلكتروني من قبل المبتزين، لكن في بعض الحالات قد يكون هناك بعض المعوقات التي تحدّ من سير القضية بالشكل الصحيح ومنها وجود المبتز في الداخل الفلسطيني وامتلاكه شريحة اتصال إسرائيلية، لذا لا يتم القبض على الجاني بشكل قانوني بسبب سيطرة الاحتلال الإسرائيلي على فضاء الاتصالات، وهذا ما تؤكده دراسة (الحقاني، 2013) بعنوان "مهارات البحث والتحقيق في الجرائم المعلوماتية- دراسة ميدانية أجريت على ضباط الشرطة بمدينة الرياض"، التي أشارت إلى وجود معوقات تحدّ من تطوير هذه المهارات في البحث والتحقيق.

أما فيما يخصّ اللجوء إلى الجهات العشائرية لحلّ جريمة الابتزاز الإلكترونيّ بطرق وديّة، فقد تبين أنّ هذا الخيار متدنٍ ولا يتم اللجوء إليه، ويعود ذلك إلى كون هذا النوع من الجرائم يحتاج إلى السريّة وإلى المتابعة من قبل جهات مختصة كوحدة حماية الأسرة، لذلك يكون الحلّ العشائري غير مقبول كونه يميل إلى الجهر والإعلان، ووجود الكثير من الأفراد، وهذا تأكيد على حصول بند وفقرة السريّة في التعامل مع مثل هذه القضايا على أعلى نسبة تحديدا في نسبة القضايا التي لها علاقة بصورة أو بأخرى بقضايا المرأة والشرف حسب المجتمعات العربيّة.

حيث تتفق هذه النتائج مع السؤال السادس في المقابلات الذي ينصّ على "ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونيّة ووحدة حماية الأسرة في الشرطة الفلسطينيّة ونيابة الجرائم الإلكترونيّة في النيابة العامة في التعامل مع جرائم الابتزاز الإلكتروني"، إذ تتمثل بإجراءات قانونية وفنية مرتبطة ارتباطا وثيقا في الجريمة وأسلوب تتبع الجاني حتى لا يلحق ضرر بالضحيّة.

مناقشة نتائج السؤال الفرعي الرابع:

ما هي الآثار الناجمة عن جرائم الابتزاز الإلكترونيّ لدى الضحايا ؟

للإجابة عن هذا السؤال تمّ حساب المتوسطات الحسابية والانحرافات المعياريّة لاستجابات أفراد عيّنة الدراسة على فقرات الاستبانة التي تعبر عن الآثار الناجمة عن جرائم الابتزاز الإلكترونيّ لدى الضحايا، حيث يلاحظ من الجدول البياني رقم (6.4) أنّ المتوسط الحسابي للدرجة الكلية (4.25) والانحراف المعياري (0.527) وهذا يدل على أنّ الآثار الناجمة عن جرائم الابتزاز الإلكترونيّ لدى الضحايا جاء بدرجة عالية.

كما وتشير النتائج في الجدول رقم (6.4) إلى أنّ جميع الفقرات جاءت بدرجة عالية. وحصلت الفقرة رقم (2) التي نصّها " التفكك اسري " على أعلى متوسط حسابي (4.51)، يليها الفقرة رقم (1) التي نصّها "انتشار الانحراف بين الضحايا والمبتزين " بمتوسط حسابي (4.45)، وحصلت الفقرة رقم (14) التي نصّها "تدني مستوى الذكاء العاطفيّ لدى الضحية" مع العلم بان الذكاء العاطفيّ يعني قدرة الفرد على مراقبة مشاعره وانفعالاته الذاتية وانفعالات ومشاعر الآخرين والموازنة بينهما حصل على

أقلّ متوسط حسابي (3.96)، يليها الفقرة رقم (15) التي نصّها "يتحول مزاج الضحية إلى مزاج حاد يصعب التعامل معه" بمتوسط حسابي (4.11).

أشارت النتائج إلى أنّ أهم الآثار التي تنتج عن الابتزاز الإلكتروني هي التفكك الأسري، وانتشار الانحراف بين الضحايا والمبتزين، كما أشارت نتائج المقابلات إلى أنّ هناك حالات تتعرض للصدمة النفسية ويمكن أن تؤدي في بعض الحالات إلى الموت.

يمكن تفسير ذلك بكون الابتزاز الإلكتروني يؤدي إلى الكثير من المشاكل، بالتالي تكون الآثار الناتجة عنه كبيرة، فالسيطرة على الضحية من خلال السيطرة والاستيلاء على الصور والمعلومات الخاصة بالضحية، من ثم بدء الابتزاز بمبالغ مالية عالية، أو مصاغ ذهبي، قد لا تستطيع الضحية توفيرها فتلجأ في الكثير من حالات الابتزاز إلى سرقة المبالغ المالية من الأهل، الذي من شأنه أن يؤثر على وضعهم المادي والأسري والاجتماعي مع الآخرين، أمّا على الصعيد الصحيّ، فقد تؤدي هذه الجرائم إلى الجلطات الناتجة عن الصدمة النفسية سواء للضحية أو لأهلها، وفي كلّ هذه الحالات تكون الآثار سلبية على الأسرة من ناحية، وعلى المجتمع كلّ من ناحية أخرى، إضافة إلى كونه في كثير من الأحيان يؤدي إلى تفكك وتشتت الأسرة، وعزل الضحية وأهلها عن المحيط ذلك لتعرضها إلى التشوية وسوء السمعة، وقد يؤدي إلى تركهم لمكان سكنهم والرحيل إلى مكان آخر بسبب ما يسمى في علم الجريمة بوصمة العار، حيث يتفق هذا مع نظرية الوصمة الاجتماعية التي ظهرت في حقبة الخمسينيات (1950-1951)، ومن أبرز روادها "الدوين ليمورت وهوارد بيكر" التي تقيد بأنّ كلّ فرد تتم إدانته بفعل مخالف للقوانين والعادات والتقاليد يتم نبذه ووصمه بالفعل الذي قام به هو وأهله، حيث يبقى هذا الفعل مرافقا له في تاريخه الاجتماعيّ، ويمكن أن نستدل على ذلك خاصة عندما تكون الضحية أنثى ويتمّ ابتزازها ابتزازا جنسياً يتم نبذها هي وأهلها، فتصل الضحية وأهلها إلى طريق مسدود فتحاول فيه التخلص من حياتها، هذا ما نستدل عليه من خلال التقرير الصحفي ل(عتمه، 2019) حيث كان الابتزاز الإلكتروني سببا في ارتفاع نسبة الانتحار في فلسطين المحتلة ممّا شكل نسبة (4%) من المجموع الإجمالي لعام (2018).

وعليه يمكن القول: إنّ هذه الجرائم تؤدي إلى تدمير الأسرة ثم المجتمع، إضافة إلى القيم والعادات والأخلاق، وتعمل على تفشي ظواهر مختلفة في المجتمعة لم تكن من قبل، كذلك تؤدي إلى رفع

مستوى الجرائم بين الأفراد، كون هذه الجريمة لا تختلف عن الجرائم الأخرى إلا بكونها تبدأ من دون وجود الجاني والضحية في مسرح الجريمة معا بسبب التطور التكنولوجي الذي أسهم في عدم وجود حدود أو مسافات من خلال شبكة الإنترنت ، هذا المبدأ يتنافى مع نظرية النشاط الرتيب التي تقوم على ثلاث عناصر أساسية (الدافعية لدى الجاني، المجني عليه المناسب، غياب الرادع والقانون).

كما تبين من النتائج أنّ مزاج الضحية لا يتحول إلى مزاج حاد يصعب التعامل معه، وهذا يعني أنّ مستوى حالات الانتحار وتحول الضحية إلى شخص مريض نفسياً كانت قليلة، فقد يكون من بين كلّ (100) ضحية تعرضت للابتزاز الإلكتروني (حالة أو حالتان) تأثرت بشكل مباشر وأدى الابتزاز فيها إلى التوجه نحو الانتحار.

ويمكن تفسير ذلك بكون الضحية في حالة الابتزاز الإلكتروني تتعرض إلى ابتزاز مادي أو عاطفي، فالعاطفي يمكن السيطرة عليه والمادي يمكن إعادة المبالغ من خلال وحدة مكافحة الجرائم الإلكترونية، وهنا تعود الضحية إلى الحياة العامة تحديداً عندما يتم التعامل مع الموضوع في سرية تامة، وهذا ما يتم العمل به داخل وحدات الجرائم الإلكترونية ووحدة حماية الأسرة، لذلك يكون تأثير الضحية بسيطاً، حيث يمكن من خلال العلاج والمتابعة من قبل الأسرة عودة الضحية إلى الحياة العامة.

وتتفق هذه النتيجة أيضاً مع نتيجة السؤال السابع في المقابلات الذي ينص على " ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على الضحايا؟"، والسؤال الثامن في المقابلات الذي ينص على " ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟"، إذ يؤكد ذلك على وجود آثار متنوعة لهذه الجريمة على الضحية أولها الآثار النفسية المتمثلة في الضغوط والتوتر وعدم النوم والتفكير بالانتحار للتخلص من الآثار الاجتماعية المتمثلة في وصمة العار التي سببتها الضحية للأسرة بسبب انتشار الصور أو الفيديوهات الخاصة بها، التي قد ينتج عنها التفكك الأسري نتيجة رفض أفراد الأسرة للضحية، والانحراف، والطلاق، والقتل في بعض الأحيان للتخلص من الفضيحة (وصمة العار) التي تلحق بالأسرة نتيجة تسريب محادثات وصور وفيديو غير لائق للضحية، وهناك آثار مادية تقع بها الضحية في حال استجابة للابتزاز المالي فينتج تكرار طلب المال من قبل الجاني، فقد تلجأ الضحية للسرقة من أسرته لتقوم بإعطاء المال للجاني حتى لا يقوم بفضحها.

مناقشة نتائج السؤال الثالث:

هل توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني؟.

يتبين من خلال الجدول البياني رقم (7.4) أنّ قيمة معامل ارتباط بيرسون للدرجة الكلية (-0.043)، ومستوى الدلالة (0.724)، أي أنه لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا، وبذلك تمّ رفض الفرضية.

يمكن تفسير ذلك بأنّ الذكاء العاطفي يتكون من عدة قدرات متنوعة (الوعي بالذات: تعني قدرة الفرد على فهم عواطفه وإدراك مشاعره وتميزها، وإدارة الانفعالات الذاتية: تعني قدرة الفرد التعامل مع المشاعر السلبية، والدافعية: تعني سعي الفرد نحو تحقيق "دوافعه" رغباته، ويتم ذلك من خلال "الأمل، المثابرة، والحماس، واستمرار السعي"، ومعرفة عواطف الآخرين وفهمها: وتعني قراءة مشاعر الآخرين وصوتهم وتعبيرات وجوههم، وإدارة الانفعالات من حلّ المشكلات والتحكم في الانفعالات)، ووفق الجدول البياني رقم (1.4) فإنّ هناك تفاوتاً في هذه المقدرات نتيجة الفروق الفردية ما بين الأفراد، حيث إنّها ليست بالضرورة أن يكون الفرد قادراً على حلّ مشكلاته التي قد تصيبه لكن بالمقابل قد يكون قادر على فهم ذاته وانفعالاته والتحكم فيها، بينما قد يملك البعض القدرة على فهم الآخرين والسيطرة عليهم دون الوعي بذاته وفهم عواطفه والتحكم بها وتميزها، لذا قد يستغل الجاني الضحية من خلال إقناعه بأنّه شخص سوي، وفي حقيقة الأمر يعاني من بعض الأمراض النفسية، هذا يتوافق مع دراسة (Sharma et al., 2015) بعنوان "العلاقة بين الذكاء العاطفي والسلوكي الإجرامي - دراسة بين المجرمين المدانين"، التي أشارت إلى أنّ مجموعة المجرمين المدانين بجرائم القتل والاغتصاب على درجات أقلّ بكثير في جميع مجالات الاستبانة مثل: الوعي داخل الذات (المشاعر الخاصة)، والتوعية بين الأفراد (عواطف أخرى)، وإدارة داخل الذات (المشاعر الخاصة) وإدارة العلاقات الشخصية (الآخرين المشاعر)، والحاصل العاطفي الكلي في مقارنته بنظرانهم العاديين، ويرتفع الذكاء العاطفي بتدني درجة الجريمة، فالجاني في قضايا القتل والاغتصاب عادة ما يكون ذا مستوى منخفض من الذكاء العاطفي، في حين أنّ المبتزين الإلكترونيين يكون لديهم مستوى أعلى من الذكاء العاطفي كونهم يستخدمون هذا الذكاء في الإيقاع بالضحية، والاستفادة منه دون أن يتضرر الجاني، لذلك يتوجه

المعالجون لمرتكبي الجرائم برفع مستوى الذكاء العاطفي لديهم ليكونوا قادرين على تقدير مشاعرهم ومشاعر الآخرين، وهذا يتفق مع دراسة (Hampson,2012)، بعنوان " دور الذكاء العاطفي في النشاط الإجرامي للشباب المشاركين في خدمة ليدز للشباب المخالفة". التي أشارت إلى أنه يجب أن يكون هناك فرصة للشباب المشتركين في خدمة ليدز لتطوير الذكاء العاطفي (المخالفين) لكي يتمكنوا من تقدير مشاعر الآخرين، وفهم عواطفهم، حيث يساعدهم ذلك على حماية أنفسهم من أي خطر تحديدا خطر الابتزاز الإلكتروني الذي من الممكن أن يكونوا أحد الجناة فيه.

أو في الحالة الثانية يكون من خلال سرقة المبتز لبيانات خاصة بالضحية والدخول على حاسوبه الخاص وسرقة الصور، ثم البدء بعملية الابتزاز الإلكتروني، في هذه الحالة أيضا لا يشترط في الضحية أن يكون على قدرة عالية من الذكاء العاطفي ليستطيع التصرف بالشكل السليم وعدم التعاطي مع المبتز، وفي حالات كثيرة تعتقد الضحية أن المبتز يسعى للحصول على المال لمرة واحدة فقط، وحتى لا تتأثر أية مشاكل حولها ترضخ لطلبات المبتز، وبالمقابل يتمتع الجاني بمستوى ذكاء عاطفي عالٍ، فيدرك أن الضحية تسعى للحفاظ على سمعة طيبة، فيكرر الطلب مرة أخرى.

هنا يمكن القول: إن مستوى الذكاء العاطفي عادة ما يكون لدى المبتز أعلى منه لدى الضحية، والدليل على ذلك أن المبتز عادة ما يكون لديه القدرة السريعة على فهم الضحية وتحديد نقطة الضعف لديه واستغلالها لتحقيق أهدافه وإخضاعها، وسلب خصوصياته ومساومتها عليها فيما بعد، حيث تُعدّ هذه نتيجة منطقية لأنه لو كانت الضحية تمتلك ذكاء عاطفي بمفهومه السابق لما تعرضت للابتزاز الإلكتروني، بالمقابل تتعرض الضحية ذات الذكاء العاطفي المتدني إلى فرصة أكبر للابتزاز الإلكتروني.

مناقشة نتائج السؤال الرابع:

هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغيرات الدراسة (الجنس، المستوى التعليمي، مكان السكن، العمر، الوظيفة، مستوى الدخل، الحالة الاجتماعية، معدل استخدام مواقع التواصل الاجتماعي)؟

(الإجابة عن هذا السؤال تمثل الإجابة عن الفرضية الرئيسية الآتية: توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($0.05 \geq \alpha$) حول ممارسة جرائم الابتزاز الإلكتروني في الضفة الغربية تُعزى لمتغيرات الدراسة التي كانت نتائجها على النحو الآتي:

• **الجنس:** توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة الباحثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير الجنس".

تم فحص الفرضية الأولى بحساب نتائج اختبار "ت" والمتوسطات الحسابية لاستجابة أفراد عينة الدراسة في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير الجنس، حيث أشارت النتائج وفق الجدول البياني رقم (8.4) إلى أنه لا توجد فروق دالة إحصائية فيما يتعلق بالجنس، أي أنه فرصة تعرض الذكور والإناث لجرائم الابتزاز الإلكتروني متساوية تقريباً، ذلك نتيجة لاختلال التركيب الاجتماعي في المجتمعات الناجم عن التطور التكنولوجي والاجتماعي الذي أضاف العديد من السلوكيات التي أصبحت متاحة لأن يقوم بها كلا الجنسين وكانت مرفوضة سابقاً مثل: نشر الصور الخاصة على مواقع التواصل الاجتماعي والحصول على العلاقات العاطفية وغيرها الكثير، نتيجة للتغيرات الحاصلة في المجتمع وضعفت القيم والأعراف والتقاليد الرادعة للسلوكيات ذلك وفق نظرية اللامعيارية أو الأنومي، بالتالي قد يجد المجتمع صعوبة في وضع وسائل الضبط الاجتماعي نتيجة لاختلاف شرائح المجتمع وانتمائهم، مما يؤدي إلى ضعف الضبط داخل الأسرة نفسها وتكسر الروابط الأسرية واتجاه بعض الأسر إلى اتباع نمط الأسرة النووية، مما أدى إلى عدم حصول الأبناء على الدعم والمتابعة الكافية، مما ينتج عنها تمزق وسائل الضبط الاجتماعي والأسري فينعكس على القيم والأعراف والعادات والتقاليد التي تسنها المجتمعات ليشبع الأفراد شهواتهم بطرق مشروعة من خلال الزواج والعمل المشروع، فينتج عن هذا التمزق محاولة لبعض الأفراد تحقيق أكبر قدر ممكن من رغباتهم وشهواتهم دون وجه وبطرق غير مشروعة، منها الجرائم الإلكترونية لتحقيق رغباتهم بطرق غير مشروعة أو استخدام الشبكة العنكبوتية للهروب من واقعه الذي لا يستطيع تغييره.

• **المستوى التعليمي:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة الباحثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير المستوى التعليمي".

تم فحص الفرضية الثانية تمّ حساب المتوسطات الحسابية لاستجابة أفراد عينة الدراسة على ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير المستوى التعليمي، حيث أشارت النتائج وفق الجدول البياني رقم (9.4) وجود فروق ظاهرية في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير المستوى التعليمي، ولمعرفة دلالة الفروق تمّ استخدام تحليل التباين الأحادي (one way ANOVA) كما يظهر في الجدول رقم (10.4)، يلاحظ أنّ قيمة F للدرجة الكلية (1.397) ومستوى الدلالة (0.254) وهي أكبر من مستوى الدلالة ($0.05 \geq \alpha$)، أي أنّه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير المستوى التعليمي، بذلك تمّ رفض الفرضية الثانية، حيث أشارت النتائج إلى أنّه لا توجد فروق دالة إحصائية فيما يتعلق بالمستوى التعليمي، أي أنّ فرصة تعرض الأفراد لجرائم الابتزاز الإلكتروني ليس لها علاقة بمستواهم التعليمي سواء كان حاصل على شهادة جامعية أو غير متعلم (دون الثانوي)، كون المقياس في هذه الحالة يعتمد بدرجة كبيرة على قدرات الشخص في التعامل مع الآخرين وفهمهم وقدرته على فهم ذاته، والجنّة عادة ما يكون لديهم القدرة على تقمص شخصيات وهمية بدرجة من عالية من الدقة ذلك لارتفاع الذكاء العاطفي لديهم وقدرتهم على إيهام الضحية بأي وضع اجتماعي وتعليمي ومادي يعيشه الجاني بشكل وهمي، وقد تنطوي على أي شخص سواء أكان متعلما أم لم يكن، لذلك فإنّ مستوى الفراسة، والقدرة على معرفة لغة الآخرين من خلال حديثهم ومن خلال تصرفاتهم وانفعالاتهم هو المفتاح في التعامل مع صدقهم أو كذبهم وليس مستواهم التعليمي.

• **مكان السكن:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة الباحثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير المستوى مكان السكن".

أشارت النتائج إلى أنّ قيمة F للدرجة الكلية (1.386) ومستوى الدلالة (0.257) وهي أكبر من مستوى الدلالة ($0.05 \geq \alpha$)، أي أنّه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير مكان السكن، وهذه النتيجة تبين أنّ فرص تعرض الضحايا للابتزاز الإلكتروني ليس لها علاقة بمكان السكن سواء أكان في مدينة أم في قرية أو في مخيم، وفي العادة فإنّ عمليات النصب والاحتيال كما ذكرنا سابقا يتم فيها استغلال الضحية باستخدام الأجهزة الإلكترونية والتطور التكنولوجي المتصلة بشبكة الإنترنت التي سهلت التواصل مع الآخرين دون حدود أو قيود جغرافية ومكانية، وهذا لا يؤثر على مكان سكن الفرد، وعادة ما يكون ذا علاقة مباشرة بقدرة الفرد على معرفة مصالح الآخرين والاحتياجات التي تنقصهم، والتي يتم توضيحها من خلال نوع

الحديث من قبل الجاني، كما أنّ مستوى الذكاء العاطفيّ يمكن أن يساعد بشكل إيجابي على معرفة نوايا الآخرين من خلال أفعالهم وكلامهم وردود الفعل، ليشكل كلّ ذلك معلومات للضحية لتكون قادرة على التصدي للجاني وحماية نفسها.

• **العمر:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكترونيّ تُعزى لمتغير العمر".

يلاحظ أن قيمة ف للدرجة الكلية (0.598) ومستوى الدلالة (0.701) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$)، أي أنه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكترونيّ تُعزى لمتغير العمر، هذا يشير إلى تماثل فرص الأفراد في الوقوع ضحايا لجرائم الابتزاز الإلكترونيّ باختلاف أعمارهم، سواء الصغار أو كبار السن، وقد تكون النوايا الحسنة للضحية في التعامل مع الجاني هي الفيصل في بناء العلاقة معه، وعادة ما تكون الوحدة أو الحاجة إلى الآخرين هي السبب في تقبل الضحية للحديث مع الجاني، فالشعور بالوحدة قد يمر به المراهقين أو كبار السنّ على حدّ سواء، بينما الجاني بشكل عام عندما يقوم بتحديد هدفه من الابتزاز الإلكترونيّ، الذي قد يكون الحصول على المال أو إشباع رغباته الجنسية أو التشهير بالضحية أو أي فرصة أخرى فإنه لا يهتم بعمر الضحية من ناحية، ولكنه يهتم من ناحية أخرى بنوع الفرصة المناسبة التي يمكن أن يحصل عليها من خلال الضحية لتحقيق أهدافه مستغلا ذكائه العاطفيّ ليكون قادرا على الوصول للضحية واكتساب ثقتها بشكل تدريجيّ.

• **الوظيفة:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكترونيّ تُعزى لمتغير الوظيفة".

يتبين من خلال الجدول رقم (16.4) إن قيمة "ت" للدرجة الكلية (0.560)، ومستوى الدلالة (0.577)، أي أنه لا توجد فروق في ممارسة جرائم الابتزاز الإلكترونيّ تُعزى لمتغير الوظيفة، هذه النتيجة أيضا تشير إلى أنّ الأفراد بغض النظر عن وظيفتهم يتمتعون بنفس الفرص للوقوع ضحية للابتزاز الإلكترونيّ، وعادة ما يكون الجناة من النوع الذي يمتلك مستوى مرتفع من الأمل والمرونة من أجل إيجاد سبل الوصول إلى أهدافهم أو تغيير الأهداف التي يستحيل تحقيقها هم يتمتعون بالذكاء العاطفيّ الذي يمكنهم من تقسيم المهام الصعبة إلى أجزاء صغيرة يمكن التعامل معها، فهم يسقطون

فشلهم على شيء ما يمكن تغييره لينجحوا فيه في المرة القادمة، بينما يلوم المتشائمون أنفسهم ويسقطون ويبررون فشلهم إلى بعض صفات دائمة هم عاجزون عن تغييرها، لذلك يستغل الجناة ذلك من خلال التعامل مع عواطف الآخرين أو ما يعرف بفن إدارة العلاقات بين البشر للوصول إلى مبتغاهم لدى الضحية التي قد تعمل بأي منصب كان بوظيفته أو قد لا يعمل حتى وفقاً لأهداف الجاني الذي يسعى ويطمح للحصول على هدفه بشكل سهل من خلال ممارسة الابتزاز الإلكتروني.

• **الدخل:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير الدخل."

يلاحظ أنّ قيمة ف للدرجة الكلية (0.484) ومستوى الدلالة (0.618) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$)، أي أنه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير مستوى الدخل، كذلك فيما يتعلق بمستوى الدخل، كون الجاني عادة ما يهتم بوجود مشكلة لدى الضحية سواء أكان ذا دخل مرتفع أم متوسط أم منخفض، كونه يرى في جميع الأشخاص القدرة على توفير المال وقت الضرورة، وهذا ما حصل في كثير من الحالات التي كان الضحية يلجأ فيها إلى الاستدانة أو بيع المجوهرات من أجل الحصول على المال للجاني، وعند الوصول إلى نقطة الصفر وعدم توفر المال، قد يلجأ الضحية للسرقة أو حتى ممارسة الفاحشة مع الجاني مقابل إسكاته، وعندما تصل الضحية إلى طريق مسدود قد تحاول اللجوء للجهات المختصة أو محاولة الانتحار، وعليه يمكن القول إن الدخل لا يكون عاملاً مؤثراً، فالجاني يركز في البداية على عواطف الضحية والمشكلات التي يمكن أن تتعرض لها في الحياة العامة، ويرى في نفسه الطبيب النفسي الذي يمكنه أن يعمل على شفاء المرضى وهنا تبدأ المشكلة.

• **الحالة الاجتماعية:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير الحالة الاجتماعية."

يتبين أنّ قيمة "ت" للدرجة الكلية (0.344) ومستوى الدلالة (0.732)، أي أنه لا توجد فروق في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير الحالة الاجتماعية، كذلك فيما يخص الحالة الاجتماعية، فلا يهتم إن كانت الضحية متروجة، عزباء، أو مطلقة، طالما في جميع الأحوال يمكن للجاني الحصول على الجنس أو المال، فكل فتاة قادرة على توفير هذا الاحتياج للجاني، وهذا ما يدفع

الجاني لعدم الاهتمام بالحالة الاجتماعية للضحية، لأنّ الجاني لديه هدف محدد يسعى إليه قد يكون مالي أو جنسي أو تشهير أو انتقام، فتكون خطته منصبة على الإيقاع بالضحية بأي طريقة كانت حتى ولو كانت من خلال اختراق جهاز الضحية دون معرفتها ذلك.

• **معدل الاستخدام لمواقع التواصل الاجتماعي:** "توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \geq 0.05$) في استجابة المبحوثين حول ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير معدل استخدام مواقع التواصل الاجتماعي".

يلاحظ أنّ قيمة ف للدرجة الكلية (1.090) ومستوى الدلالة (0.359) وهي أكبر من مستوى الدلالة ($\alpha \geq 0.05$)، أي أنّه لا توجد فروق دالة إحصائية في ممارسة جرائم الابتزاز الإلكتروني تُعزى لمتغير معدل الاستخدام لمواقع التواصل الاجتماعي، إنّ التعرض للابتزاز الإلكتروني لا يتأثر بكثرة الولوج إلى الإنترنت واستخدام مواقع التواصل الاجتماعي، فقد يتعرض الضحية إلى الابتزاز الإلكتروني مع أول مرة يستخدم فيها مواقع التواصل الاجتماعي، وبنفس النسبة يمكن أن يقع مدمن مواقع التواصل الاجتماعي، وهنا يكمن الحديث عن طبيعة الأهداف التي يبحث عنها الجاني، ويختار البيئة المناسبة والظروف التي تعيشها الضحية، ثم تبدأ بعدها عملية التخطيط للابتزاز الإلكتروني، وهذا يحدث بعد عدة مرات من التواصل بين الطرفين، فقد لا تتوفر الشروط المطلوبة من قبل الجاني في الضحية، وعندها يلغي الجاني عملية التواصل ثم يبدأ في البحث عن ضحية أخرى، لذلك لا يعد معدل استخدام المواقع الإلكترونية ومواقع التواصل بشكل خاص مؤثراً في الوقوع في الجريمة.

مما سبق يمكن القول: إنّ المتغيرات الديمغرافية لا تؤثر في اختيار الجاني للضحية، وليست من ضمن الأهداف التي يبحث عنها، وإنما يكون البحث بشكل مناسب ضحية تعاني من فراغ عاطفي، أو لديها مشكلات أسرية، أو تعاني من نقص في التواصل مع الآخرين، وهذا يتوافق مع نظرية الفرصة التي تؤكد أنّ الجاني تتوفر لديه الرغبة في القيام بالجريمة، ولكنه عادة ما يبحث عن الفرصة المناسبة (أي الضحية التي تتناسب مع أهدافه)، ثم يستغل عدم وجود قوانين رادعة وغياب الرقابة على مواقع التواصل الاجتماعي لكون هذه المواقع توفر الخصوصية لأفرادها من خلال الحديث الخاص، فيعمل على استغلال ذلك للإيقاع بالضحية وابتزازها لعدة مرات.

2.5 مناقشة النتائج المتعلقة بالمقابلات:

تكمن أهم نتائج المقابلات التي تمت مع العاملين في وحدات الجرائم الإلكترونية في جهاز الشرطة الفلسطينية والنيابة العامة ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية فيما يلي:

○ السؤال الأول: هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟

أشارت النتائج الخاصة بالمقابلات إلى أنّ مستوى الذكاء العاطفي يؤثر على زيادة ممارسة جرائم الابتزاز الإلكتروني، ويعود ذلك إلى اعتبارهم أنّ الذكاء العاطفي للمجرم كلما زاد، زادت قدرته على فهم مشاعر الضحية، والقدرة على التحكم بمشاعره، تحديداً لقدرته على تكوين فهم صحيح لطبيعة الحياة الأسرية التي يعيشها، فإذا كان هناك تفكك أسري، أو وحدة وعزلة ذاتية، أو لم يكن لدى الضحية أصدقاء، أو كان يعاني من العنف داخل الأسرة، فإن الجاني في هذه الحالة سيعمل على توفير كلّ المعلومات والبيانات الخاصة به، وعليه يكون لديه فرصة لبدء البحث عن الطرق التي يمكن استغلالها للوصول إلى قلب الضحية، وهو ما يشير إليه (جولمان، 2000) في أنّ القدرة على بذل الجهود من قبل الأفراد ذوي الإمكانيات العقلية العالية، الذين يتمتعون بمهارات المفاوضات والقدرة على إيجاد حلول مناسبة للمشكلات التي تواجه الأفراد وطرحها، والتي يمكن من خلالها السيطرة عليهم، ومحاولة مساعدتهم في حلّ هذه المشكلات، حيث إنّ مهارة التعاطف والتواصل تسهل القدرة على المواجهة، أو التعرف على مشاعر الناس واهتماماتهم بصورة مناسبة. أنّه فنّ العلاقات بين البشر، وعادة ما يكون لدى الجاني القدرة على بناء تصورات أولية لضحيته من خلال بعض الصور والكتابات التي تكون منشورة على الصفحات الخاصة به في مواقع التواصل الاجتماعي، ومن خلال تحليل الصور والكتابات يمكن التوصل إلى الحالة النفسية والاجتماعية والعاطفية والثقافية للفرد، والذي سيكون فيما بعد الضحية، إذ يتم إيهامه بقدرته على فهم وتحليل شخصيته، ومعرفة طبيعة تفكيره، وأنّه - أي الجاني - يعاني من نفس الظروف التي يعيشها الضحية، وذلك لتسهيل اكتساب التعاطف العام له.

ويوضح جولمان أيضا أنّ هناك العديد من الأساليب العاطفيّة الأبوية الشائعة مثل تجاهل المشاعر حيث ينظر الآباء إلى القلق العاطفيّ على أنّه ممل وتافه، يجب أن ينتظروا حتى ينتهي من تلقاء نفسه هؤلاء الآباء يفشلون في استغلال لحظات الطفل العاطفيّة كفرصة يتقربون فيها من الطفل أكثر، أو لكي يساعده على تعلم الكفاءة العاطفيّة، وفي هذا السياق يمكن التوصل إلى نتيجة بأنّ برود المشاعر الأبويّة للأبناء يساعد في اقتناص الجاني لفرصة لعب دور الشخص القادر على إعطاء هذه المشاعر والحنان والعاطفة للضحية، والذي يكون بحاجته نتيجة لفقدانه في الأسرة التي يعيش فيها، حيث يتفق هذا مع نظريّة الفرصة التي تعتمد على ثلاثة مكونات أهمها الضحية المناسبة التي يجدها بأنّها فرصة متاحة وسهلة له لضعفها وعدم قدرتها الدفاع عن نفسها نتيجة فقدانها العاطفة في أسرتها، ومن ثم يستغل غياب الرقابة على الشبكة العنكبوتيّة (الإنترنت) للإيقاع بها بعلاقات غير شرعية تنتهي غالبا بالابتزاز والتهديد.

السؤال الثاني: ما هي أكثر أنواع جرائم الابتزاز الإلكترونيّ التي تتعاملون معها في مجال عملكم؟

تشير نتائج المقابلات إلى أنّ الابتزاز المالي هو الأهم في سلسلة الابتزازات التي يقوم بها الجاني، ثم يليه الابتزاز الجنسي، ويمكن تفسير ذلك بأنّ الجاني في سبيل الحصول على المال بالدرجة الأولى يحاول الحصول على كافة البيانات الخاصة بالضحية، فإذا كانت البيانات ذات صلة مباشرة به كحسابات بنكية، أو أوراق ثبوتية مهمة، أو محادثات مع آخرين، أو صور وفيديوهات يكون هنا قد حصل على ما يريد بسهولة من خلال البحث في جهاز الضحية، أمّا في حال لم يستطع الحصول على هذه البيانات فيكون اللجوء إلى استخدام العاطفة كوسيلة للسيطرة على الضحية، والحصول على البيانات اللازمة التي سيتم استخدامها فيما بعد من قبل الجاني، كالصور والفيديوهات الخاصة، في المرحلة الأولى يكون الابتزاز الجنسيّ بعد استغلاله حاجة الضحية إلى الجنس، ثم في المرحلة التالية يعمل على استخدام هذه البيانات من أجل الحصول على المال، وهو ما تشير إليه دراسة (الجروي، 2011)، بعنوان "العوامل الاجتماعيّة والثقافيّة المؤدية لظاهرة ابتزاز المرأة"، إذ تبين أنّ أهم دوافع الابتزاز لدى المبتز هو إشباع رغباته

الجنسية، من أكثر أنواع الابتزاز انتشارا (الجنسي، والنفسي، والمادي، العاطفي)، وعادة ما يبحث المبتز عن الجانب المادي لدى الضحية، ويكون ذلك من خلال الجانب الجنسي بالدرجة الأولى.

واستنادا إلى (كرسوع، 2016) فإنّ الجاني في أغلب الأحيان يكون من ذوي الدخل المحدود، أو يعاني من البطالة والفقر، لذلك يتجه إلى استخدام الوسائل غير المشروعة للحصول على المال من خلال معاينة بعض الأشخاص ذوي الدخل المرتفع، أو أصحاب المصانع والشركات، أو النساء كونهن يمتلكن مصاغا ذهبيا، فمن خلال السيطرة على الضحية يمكن للجاني الحصول على المال وتحسين وضعه المادي، كذلك يمكن أن يكون الهدف الذي يسعى إليه الجاني هو الانتقام من الضحية بسبب خلافات قديمة قد تكون عاطفية أو مادية، فيكون الابتزاز نابعا من الحقد والبغض للضحية، ويكون من وجهة نظره تحصيلًا للحق الذي لم يستطع الحصول عليه بالطريق المشروع.

وبالاعتماد على إحصائيات (الجهاز المركزي للإحصاء الفلسطيني، 2017) فإنّ معدل الفقر وفقا لخط الفقر في قطاع غزة يشكل (53%) من إجمالي السكان بينما في الضفة الغربية (13.9%).

○ السؤال الثالث: ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟

أشارت نتائج المقابلات إلى أن أهم الوسائل المستخدمة للإيقاع بالضحية هي الحصول على البيانات المختلفة منه، سواء من خلال الاختراق، أو من خلال بناء جسور الثقة المتمثلة في العلاقة العاطفية، أو الإيهام بالمساعدة في الحصول على وظيفة، أو زواج، أو من خلال المساعدة في حلّ مشكلات أخرى تعاني منها الضحية، حيث يمثل ما سبق معلومات هامة له، يرى فيها الجاني وسيلة للحصول على ما يريد من الضحية من الصور والفيديوهات الخاصة بها، سواء من خلال العلاقة مع الجاني نفسه، أو من خلال اختراق جهازه الشخصي والحصول عليها دون علم الضحية، كذلك في الحصول على البيانات الشخصية من خلال الإيهام بتوفير فرص عمل، فيتم الحصول على السيرة الذاتية والهوية الشخصية والمعلومات الخاصة، التي تساعده

لابتزاز الضحية فيما بعد، أو قد يكون ذلك من خلال معرفة الجاني لعلاقة الضحية بشخص أو بعدة أشخاص آخرين والحصول على المحادثات الخاصة بهم ثم استخدامها في جريمة الابتزاز. يمكن القول: إن هذه الوسائل التي يتم استخدامها عادة ما تكون ضمن العلاقة غير الشرعية بين الضحية والجاني، وعادة ما تمكن الضحية الجاني من خلال الإهمال من الحصول على المعلومات والبيانات الخاصة بها، وهذا يؤدي إلى سرقة هذه البيانات أو استخدامها فيما بعد من أجل تهديد الضحية وابتزازها إذا رفضت القيام بما يطلبه منها، وهو ما أشارت إليه دراسة (العميرة، 2012)، بعنوان "تجريم جرائم ابتزاز النساء- دراسة تأصيلية تطبيقية"، التي بينت أن أغلب جرائم الابتزاز الإلكتروني تحدث بسبب وجود علاقة عاطفية بين الرجل والمرأة خارج إطار الزوجية، تتحمل المرأة المسؤولية الأكبر في أغلب جرائم الابتزاز الإلكتروني حيث إنها السبب للوصول إلى صورها ومستندات السرية إلى يد المبتز، حيث تقدمه ببعض الأحيان للمبتز بسبب ارتفاع مستوى الثقة أو إساءة الاستخدام التقني أو الإهمال.

وهو أيضا ما أشارت إليه دراسة (الشمراي، 2011) بعنوان "ظاهرة الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي"، حيث تتفق من حيث الوسائل المستخدمة في عملية الابتزاز وهي التهديد بنشر صور ومحادثات ورسائل عن طريق الهاتف المحمول، كما تعدّ مواقع التواصل الاجتماعيّ من الوسائل التي ساعدت على ظهور جريمة الابتزاز الإلكترونيّ كونها أسهمت في بناء أنظمة تساعد على بناء علاقات بين الأفراد من خلال أنظمة المحادثات المرئية والمسموعة، كما أنّ لهذه المواقع دورا في عمليات التشهير من خلال استخدام الجاني لها في التشهير بالضحية، وهو ما يتفق مع (دراسة المحمود، 2014) بعنوان "المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعيّ الحديثة- دراسة تأصيلية تطبيقية"، التي أشارت إلى أنّ هناك إيجابيات وسلبيات لاستخدام مواقع التواصل الاجتماعيّ، حيث تُعدّ مواقع التواصل الاجتماعيّ مساهمة بشكل كبير بانتشار الجرائم الإلكترونيّة كونها تستخدم من قبل الجاني لابتزاز والتهديد والتشهير إذا لم تستجب الضحية له.

○ السؤال الرابع: ما الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟

أشارت نتائج المقابلات إلى أنّ الجهل الاجتماعيّ وقلة الوعي، وعدم الحفاظ على الخصوصية في التعامل مع الأجهزة الإلكترونيّة، وعدم وجود هيئات قضائيّة متخصصة، إضافة إلى الوضع المادي السيء، وكذلك انتشار الشرائح الإسرائيليّة والإنترنت من مزود خدمة من إسرائيل لا يكون عليها رقابة فلسطينيّة، وأيضا الضغط والمشاكل الأسريّة، والفراغ العاطفيّ هي من الأسباب التي تؤدي إلى حدوث جريمة الابتزاز، ويمكن تفسير هذه النتيجة بأنّ ضعف مستويات المعرفة باستخدام مواقع التواصل الاجتماعيّ بشكل سليم، إضافة إلى الثقة المطلقة التي يوليها الأفراد الذين يستخدمون هذه المواقع في التعارف والتسلية، وعدم الاهتمام بحفظ البيانات خارج أجهزة الحاسوب والهاتف المحمول، والثقة بعدم قدرة الأفراد الآخرين على الوصول إلى البيانات أسهم في سهولة وقوعهم ضحية للابتزاز الإلكترونيّ، كذلك وجود الكثير من أوقات الفراغ لدى الأفراد واستخدامهم لهذه المواقع بشكل مستمر ويومي، ساعد في بناء علاقات مع الآخرين دون الاهتمام بمعرفتهم بالشكل السليم، وعادة ما يقوم الجاني في مثل هذه الحالات بإخفاء هويته الحقيقية وانتحال هوية أخرى لفرد يمتلك الكثير من الصفات الإيجابية التي يمكن من خلالها الإيقاع بأي شخص، فالشخصيات المثاليّة عادة ما يبحث عنها أغلب الأفراد في المجتمع، وهي الشخصية التي تحمل المؤهل العلمي العالي، والتي تتمتع بمظهر خارجي جميل، حيث يقوم الجاني بإقناع الضحية بأنّه من ذوي الدخل العالي حتى يحصل على ثقته بعدم رغبته في الحصول على المال، أو الجنس، أو العاطفة، أو الشهرة، أو غيرها من الأمور، ومع توفر كلّ هذه الصفات في الجاني، يصبح من السهل عليه إقناع الضحية في قدرته على مساعدته سواء في الزواج، أو في الحصول على فرصة عمل، أو في الصداقة البريئة التي تهدف إلى مساعدة الضحية في حلّ مشكلاتها من خلال تقديم الاستشارات لمساعدتها.

كذلك من الأسباب التي توصلت إليها الدّراسة من خلال المقابلات استخدام الشرائح الإسرائيليّة في جريمة الابتزاز الإلكترونيّ، يعتبر هذا السبب من الأسباب السياسيّة باعتبار أنّ الشرطة

الفلسطينية لا تستطيع مراقبة أو متابعة الشرائح الإسرائيلية، الأمر الذي يساعد في هروب الجاني بعد قيامه بابتزاز الضحية، وهي من الأسباب المهمة في فلسطين كونها تحول دون تحقيق العدالة، وكونها تساعد في انتشار الجريمة وعدم القدرة على حماية الأفراد في المجتمع الفلسطيني. أيضا من الأسباب الأخرى هي الظروف الاجتماعية والاقتصادية الصعبة التي يمر بها أبناء الشعب الفلسطيني بسبب مستويات العمل المتدنية، وارتفاع مستوى البطالة والفقر لدى الكثير من الأفراد، تحديدا في القرى والمخيمات، وهذا يؤثر على الاستقرار الأسري ويساعد في العديد من المشاكل الأسرية لعدم قدرة رب الأسرة على توفير الاحتياجات الأساسية للأسرة، الأمر الذي قد يؤدي إلى التفكك الأسري، أو إلى البحث عن العلاقات غير المشروعة من أجل الهروب من الواقع الأسري المعاش، إذ يؤدي ببعض الأحيان إلى إدمان الأفراد على الإنترنت والجلوس لأوقات طويلة، مما يعرضهم لخطر جرائم الابتزاز، كونهم فقدوا أدوات التواصل المباشر، واعتمدوا فقط طريقة التواصل الإلكتروني، وهذا يتفق مع دراسة (الحمصي، 2009)، بعنوان "إدمان الإنترنت عند الشباب وعلاقته بمهارات التواصل الاجتماعي، دراسة ميدانية على عينة من طلاب جامعة دمشق"، وأشارت الدراسة إلى وجود علاقة بين مهارات التواصل الاجتماعي وإدمان الإنترنت تبعا للعديد من المتغيرات التي تؤثر على طبيعة الإدمان.

ويمكن تفسير ذلك أيضا بكون التقدم الحضاري والتكنولوجي السريع، أضعف قدرة الأفراد على التلاؤم والتوافق مع هذا التطور، ومعرفة كافة طرق التعامل معه، مما أضعف مستويات القيم الاجتماعية والأخلاقية، وأسهم في توجه الأفراد نحوه دون ضوابط، هذا يتفق مع ما نصت عليه النظرية اللامعيارية في أنّ "اختلال التركيب الاجتماعي الناجم عن التطور الحضاري والتكنولوجي، تضعف القيم والأعراف والتقاليد والمعتقدات الرادعة للسلوك المنحرف في المجتمع، الأمر الذي أسهم في ظهور هذا النوع من الجرائم بشكل غير مسبوق مما يعني ظهور العديد من، التأثيرات السلبية على الفرد والمجتمع.

○ السؤال الخامس: هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017) على التقليل من نسبة جرائم الابتزاز الإلكتروني، كيف ذلك؟

أشارت نتائج المقابلات إلى أنّ القانون رقم (16) لعام (2017) عمل على التقليل من الجرائم الإلكترونية بشكل عام وجرائم الابتزاز الإلكتروني بشكل خاص، ذلك لامتلاكه مقومات تقوم على ردع الجاني وعقابه من خلال وضع عقوبات وغرامات مالية مقابل كلّ فعل غير قانوني يقوم به بانتهاك خصوصية غيره أو بممارسة الابتزاز والتهديد والتشهير سوء للفرد أو المجتمع أو المؤسسات، إضافة إلى حماية الضحية من خلال إجراءات قانونية وفنية متبعة في هذه القضايا، ولكن، كان هناك العديد من التحديات والصعوبات التي تحدّ من فعاليته بشكل كبير إلا وهي انتشار الشرائح الإسرائيلية، وعمل العديد من المؤسسات الحقوقية والإعلامية على عدم تنفيذ القانون بشكل كامل، حيث تُعدّ هذه النتيجة من وجهة نظر العاملين في الجهات المختصة إذ تُعدّ وجهة نظر قانونية بحته بعيدا عن أرض الواقع المتمثل في الإحصائيات التي تفيد بأن نسبة الجرائم تضاعفت تقريبا في عام (2017) حيث كان عدد الشكاوي (1327) مقارنة بعام (2018) لتشكل عدد الشكاوي (2568)، حيث تتفق هذه النتيجة مع دراسة المطيري (2015)، بعنوان "المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي-دراسة مقارنة"، التي أشارت هذه الدراسة إلى وجود فجوة تشريعية بين دول العالم فيما يتعلق بمكافحة جرائم الإلكتروني مما أدى إلى زيادة هذه الجرائم، وصعوبة تتبع أثر الجاني إذا كان خارج الحدود الجغرافية بسبب اختلاف الجوانب الإجرامية في العالم واختلاف دوافع وأساليب الجاني.

○ السؤال السادس: ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة" في التعامل مع جرائم الابتزاز الإلكتروني؟

أشارت النتائج إلى أنّ الإجراءات المتبعة من وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في التعامل مع جرائم الابتزاز الإلكتروني تمثلت في إجراء إداري مرتبط بالقانون، كذلك بإجراءات فنية مرتبطة بطرق تتبع الجاني من خلال البرامج المختصة، كذلك في سماع الشكاوي والتحقيق في الواقعة وتحديد الاحتياجات والنتائج حسب الاختصاص.

وتعدّ هذه الإجراءات مهمة في عملية ملاحقة الجاني ومتابعته، بعد تقديم الضحية بشكوى من أجل التحقيق فيما تعرضت له، وتتفق هذه النتيجة مع دراسة (الحقاني، 2013) بعنوان "مهارات البحث والتحقيق في الجرائم المعلوماتية- دراسة ميدانية أجريت على ضباط الشرطة بمدينة الرياض"، حيث أشارت الدراسة إلى ضرورة توافر المهارات العامة اللازمة للبحث والتحقيق في الجرائم المعلوماتية، كون هذا يساعد في تحقيق العدالة بالقبض على الجاني ومعاقبته بشكل رادع حتى لا يعود إلى الفعل مرة أخرى، في حين أشارت نتائج المقابلات إلى أنّ وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة يستقبلون الضحية ويعملون على توثيق بيانات الحالة من خلال شكوى تقوم الضحية بتقديمها، وتخضع كافة المعلومات المقدمة من قبل الضحية للسرية التامة، ثم يتم المحافظة على الضحية من التعرض للخطر سواء من الجاني أو الأسرة، بعد ذلك تبدأ إجراءات التدخلات الاجتماعية والنفسية المناسبة من خلال تقديم الدعم النفسي والعلاج النفسي إذا تطلب الموضوع ذلك، وإذا ما شكلت هذه الجريمة خطراً على حياة الضحية من قبل الأهل يتمّ التدخل اجتماعياً عن طريق العرف العشائري لمنع حدوث أي ضرر للضحية ويكون ذلك بمساعدة وحدة حماية الأسرة.

○ السؤال السابع: ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على الضحايا؟

أشارت نتائج المقابلات إلى وجود آثار لهذه الجريمة حيث يؤدي ذلك إلى التفكك الأسري الناتج عن رفض أفراد الأسرة للضحية بعد ما تعرضت له، في بعض الأحيان يؤدي إلى تفكير الضحية بالانتحار للتخلص من وصمة العار التي سببتها للأسرة بسبب انتشار الصور أو الفيديوهات الخاصة بها، كذلك يمكن أن ينتج عن ذلك صدمات نفسية، وحالات اكتئاب، وضعف مستويات الثقة بالنفس لدى الضحية في حال تعرضت للابتزاز من خلال الاختراق الإلكتروني لصفحتها الإلكترونية، كذلك هناك آثار مادية تقع بها الضحية في حال التعرض للابتزاز المالي نتيجة للطلب المتكرر للمال من قبل الجاني، إضافة إلى تأثيرها العاطفي على الضحية الذي قد ينتج عنه الانسحاب الاجتماعي وعدم الرغبة في الانخراط في المجتمع، ومشاعر الخوف والحزن نتيجة الضغوطات التي يمارسها الجاني عليها، وتتفق هذه النتيجة مع دراسة (Elipe, Merchan and, Ruiz,Casas, 2015), بعنوان "الذكاء العاطفي المتصور كمتغير وسيط بين الجرائم الإلكترونية وتأثيرها العاطفي". حيث أشارت النتائج إلى تأثير الجرائم الإلكترونية على الفرد في العديد من المجالات مثل: الأداء الأكاديمي، والاندماج الاجتماعي، واحترام الذات، ومما ينتج عنها مشاعر تتراوح بين الغضب والحزن لمشاكل أكثر تعقيدا مثل الاكتئاب.

كذلك تتفق هذه النتيجة مع دراسة (كردي، 2009) بعنوان "الاكتئاب والذكاء الانفعالي لدى عينة من مدمنات الشبكة العنكبوتية - دراسة وصفية مقارنة"، التي أشارت إلى أن الطالبات المدمنات أكثر اكتئابا من الطالبات غير المدمنات على استخدام الشبكة العنكبوتية ومواقع التواصل الاجتماعي، كما وأظهرت فروقا دالة في الذكاء الانفعالي بين المدمنات وغير المدمنات يساوي (11،94) أي غير المدمنات أكثر ذكاء عاطفياً من المدمنات على الشبكة العنكبوتية، كون غير المدمنات لديهن القدرة على التحكم باستخدام الشبكة العنكبوتية بما يتناسب مع أوقات الفراغ، وهذا يقلل من مستوى الإدمان على استخدام المواقع الخاصة بالتواصل الاجتماعي التي هي أساس تعرضهن لأن يكن ضحايا الابتزاز الإلكتروني، إضافة لذلك تتفق هذه النتيجة أيضا مع دراسة (الخمشي، 2010) بعنوان "الآثار الاجتماعية السلبية لاستخدام الفتاة مرحلة المراهقة للإنترنت"،

التي أشارت إلى شعور الفتاة بأنها غير راضية عن حياتها ومظلومة خاصة فيما يتعلق بعلاقتها الأسرية ورغبتها في الحصول على العاطفة وسدّ الفراغ الذي تعيشه، يؤدي إلى زيادة استخدامها للإنترنت ومواقع التواصل الاجتماعيّ، الأمر الذي يزيد من احتمالية أن تكون ضحية الابتزاز الإلكترونيّ فيما بعد.

○ السؤال الثامن: ما الآثار الناجمة عن جرائم الابتزاز الإلكترونيّ على المجتمع؟

أشارت نتائج المقابلات إلى أنّ الآثار الناجمة عن جرائم الابتزاز الإلكترونيّ على المجتمع تمثلت في زيادة في المشكلات الاجتماعية المختلفة التي يمكن أن تؤدي إلى التفكك الأسريّ، والانحراف، كالعلاقات غير الشرعية، والتوجه نحو المخدرات، والتسرب المدرسيّ، وحالات السرقة وغيرها من الجرائم الأخرى، إضافة إلى ذلك قد تصل الخلافات بين أهل الجاني والضحية إلى هدر دم الجاني، أو بالعقاب المجتمعيّ المسمى بالجلوة الذي ينتج عنه ترك البيوت والممتلكات والرحيل لأماكن أخرى دون الرجوع إلى المنطقة، كما أنّها تؤثر على القيم المجتمعية التي تغيرت بالتقدم التكنولوجيّ والعولمة، وانقلاب العالم الافتراضي المتمثل في شبكة الإنترنت إلى عالم حقيقي له قوانينه التي ألغت مستويات القيم والعادات التقليدية، كما أنّ هذه الجرائم أسهمت في ضعف مستويات الأمان المجتمعيّ لدى الأفراد، وبالتالي ضعف التعامل معه، لعدم ثقة المجتمع بالمواقع الإلكترونية، وهذا يؤثر على التجارة الإلكترونية، وعلى الخدمات الإلكترونية المقدمة من البنوك والمؤسسات.

○ السؤال التاسع: ما هي الصعوبات التي تحدّ من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

أشارت النتائج إلى أنّ أهم الصعوبات التي تحدّ من عمل وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة تتمثل في ضعف مستوى الإمكانيات المادية لعدم تخصيص مبالغ كافية في هذا المجال، بالتالي عدم وجود أجهزة

حديثه، وطواقم مدربة ومؤهلة للتصدي للجناة في هذه الجرائم، كون مرتكبي الجرائم الإلكترونية لديهم مستوى ذكاء عاطفي مرتفع.

كما أشارت النتائج إلى ضعف التعاون الدولي والتنسيق مع الجهات الخارجية المختصة في ملاحقة الجناة في جرائم الابتزاز الإلكتروني، تحديدا إذا كانوا من خارج فلسطين، كذلك ضعف التواصل مع الجهات الإسرائيلية إذا كان هناك من الجناة من يستخدم الشرائح الإسرائيلية أو يقطن في المناطق المحتلة عام (1948) في ابتزاز الضحية، وتتفق هذه النتيجة مع ما ورد في الإطار النظري فيما يخص العديد من الصعوبات التي تواجه جهات الاختصاص المتمثلة في وحدتي الجرائم الإلكترونية وحماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة في دولة فلسطين المحتلة، إذ تمثلت في عدم رصد ميزانية كافية لتوفير دورات تقوم بإكساب العاملين المهارات الفنية والتقنية، وصعوبة التنسيق مع دول أخرى عندما يكون المبتز من خارج حدود فلسطين.

3.5 ملخص النتائج :

فيما يلي استعراض لمخلص نتائج كل من الاستبانة والمقابلة الخاصة في الدراسة:

1. مستوى الذكاء العاطفي لدى ضحايا جرائم الابتزاز الإلكتروني جاء بدرجة متوسطة حسب استجاباتهم لفقرات الاستبانة.

2. أهم الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني هي العلاقات العاطفية، بينما أشارت نتائج المقابلات إلى أن أهم الوسائل المستخدمة للإيقاع بالضحية هي الحصول على البيانات المختلفة منه، سواء من خلال الحصول عليها من خلال الاختراق، أو من خلال بناء جسور الثقة المتمثلة في العلاقة العاطفية.

3. أهم الأسباب التي تؤدي إلى جرائم الابتزاز الإلكتروني هي الاختلاط بأصدقاء السوء، بينما أشارت نتائج المقابلات إلى أن الجهل الاجتماعي وقلة الوعي، وعدم الحفاظ على الخصوصية في التعامل مع الأجهزة الإلكترونية وأيضاً الضغط والمشاكل الأسرية والفراغ العاطفي هي من الأسباب التي تؤدي إلى حدوث جريمة الابتزاز.

4. إن وحدة الجرائم الإلكترونية، ووحدة حماية الأسرة في الشرطة الفلسطينية، ونيابة الجرائم الإلكترونية في النيابة العامة تتعامل مع جرائم الابتزاز الإلكتروني بدرجة عالية من السرية، بينما أشارت نتائج المقابلات إلى أن هذه الإجراءات تمثلت في إجراء إداري مرتبط بالقانون، كذلك بإجراءات فنية مرتبطة بطرق تتبع الجاني من خلال البرامج المختصة للحفاظ على سرية الضحية وعدم لحاق الضرر بها.

5. التفكك الأسري وانتشار الانحراف بين الضحايا والمبتزين من أهم الآثار الناجمة عن جرائم الابتزاز الإلكتروني على الضحايا، بينما أشارت نتائج المقابلات إلى وجود آثار لهذه الجريمة حيث تتمثل في التفكك الأسري الناتج عن رفض أفراد الأسرة للضحية بسبب ما تعرضت له، إضافة إلى تفكير الضحية بالانتحار في بعض الأحيان.

6. لا توجد علاقة ذات دلالة إحصائية عند مستوى الدلالة (0.05) بين مستوى الذكاء العاطفي وممارسة جرائم الابتزاز الإلكتروني لدى الضحايا، بينما أشارت نتائج المقابلات أن مستوى الذكاء العاطفي المرتفع للجاني يؤثر على زيادة ممارسة جرائم الابتزاز الإلكتروني وانخفاض مستوى الذكاء للضحية يُعرضها للابتزاز الإلكتروني.

7. لا توجد فروق دالة إحصائية فيما يتعلق بالمتغيرات الديموغرافية في الدراسة (الجنس، والمستوى التعليمي، ومكان السكن، والعمر، والوظيفة، والدخل، والحالة الاجتماعية، ومعدل استخدام مواقع التواصل الاجتماعي).

8. أهم الصعوبات التي تحدّ من عمل وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة تتمثل في ضعف مستوى الإمكانيات المادية، وعدم وجود أجهزة حديثة وطواقم مدربة ومؤهلة للتصدي للجناة في هذه الجرائم، تحديداً في الحالات التي يكون بها الجاني لديه مستوى ذكاء عاطفي مرتفع.

9. الابتزاز المالي هو الأهم في سلسلة الابتزازات التي يقوم بها الجاني، ثم يليه الابتزاز الجنسي.

10. أشارت نتائج المقابلات إلى أنّ الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع تمثلت في زيادة المشكلات الاجتماعية المختلفة التي يمكن أن تؤدي إلى (التفكك الأسري، والانحراف كالعلاقات غير الشرعية، التوجه نحو المخدرات، التسرب المدرسي، حالات السرقة) وغيرها من الجرائم الأخرى.

11. أشارت المقابلات إلى أنّه تمّ سنّ قانون رادع للجرائم الإلكترونية، إضافة إلى تعديله لاحقاً ومع ذلك هناك تزايد في ارتكاب الجرائم الإلكترونية.

4.5 التوصيات:

لعل ما يمكن أن توصي به الدراسة ما يلي:

1. العمل على رفع مستوى الوعي الوقائي لدى جميع أفراد المجتمع حول جرائم الابتزاز الإلكتروني، ذلك من خلال البرامج التليفزيونية والنشرات الإرشادية من قبل الشرطة الفلسطينية والنيابة العامة، ليكون لدى المواطن الوعي الكافي بوجود مثل هذه الجرائم في المجتمع.
2. رفع مستوى الثقة بالنيابة العامة والشرطة الفلسطينية وأجهزة القضاء الفلسطيني، من خلال تطبيق القانون الخاص بالجرائم الإلكترونية المعدل ونشر جلسات المحاكمة لأفراد المجتمع من خلال وسائل الإعلام المختلفة لتكون رادعا للجناة، وتحقيق الثقة للأفراد.
3. تعزيز مستوى الوعي لدى الأفراد الذين يستخدمون مواقع التواصل الاجتماعي بشكل مستمر بضرورة إبلاغ رجال الشرطة من خلال وحدة الجرائم الإلكترونية باستخدام الرقم الموحد عن أية حالة مشبوهة حتى لا يتعرض الأفراد للابتزاز من الجناة.
4. ضرورة اهتمام الأفراد المستخدمين للشبكة العنكبوتية بعمل فحص دوري لأجهزتهم، وتثبيت برامج الحماية المرخصة من قبل شركات الإنترنت الفلسطينية، وعدم استخدام الحسابات الخاصة بهم في الأماكن العامة غير الموثوقة حتى لا يتعرضوا للابتزاز الإلكتروني.
5. ضرورة توعية المواطنين واكتساب ثقتهم في أهمية عمل وحدة حماية الأسرة في جهاز الشرطة الفلسطينية فيما يتعلق باحتواء وحماية الأفراد الذين تعرضوا للابتزاز الإلكتروني ومساعدتهم من خلال تقديم الدعم النفسي والاجتماعي اللازمين لهم ولأسرهم لتجاوز هذه الأزمة وتقادي بعض من الآثار المترتبة عليها.
6. رفع مستوى الرقابة الذاتية والمجتمعية على الأبناء من قبل الأهل حتى لا يكونوا ضحايا للابتزاز الإلكتروني.
7. ضرورة عمل المزيد من الدراسات حول الضحية والجاني فيما يتعلق بالابتزاز الإلكتروني في فلسطين، لتكون مصدرا للباحثين والجهات المختصة.

8. ضرورة تخصيص ميزانيات لمكافحة الجرائم الإلكترونية لتذليل الصعوبات التي تواجه الجهات المختصة، من خلال توفير أحدث الأجهزة والبرمجيات وتدريب العاملين في وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة للتصدي للجناة، وإكسابهم مهارات التعامل مع الضحايا والجناة.
9. التشبيك والتنسيق مع المؤسسات المجتمعية والحكومية العاملة في مجال الصحة النفسية لمكافحة آثار الجرائم الإلكترونية المتمثلة في التفكك الأسري، والانحراف، والعلاقات غير الشرعية، والمخدرات، والتسرب المدرسي.
10. التطبيق الفعلي لقانون الجرائم الإلكترونية حتى يكون هناك رادع أمام الجناة عند التفكير بارتكاب هذا النوع من الجرائم.

قائمة المصادر والمراجع

أولاً: المصادر والمراجع العربية:

القران الكريم.

أبكر، سليمان مصطفى (1999). جرائم الحاسوب وأساليب مواجهتها، الرياض: أكاديمية نايف للعلوم الأمنية.

ابن منظور، جمال الدين محمد بن مكرم (1990). لسان العرب، بيروت: دار صادر.

أبو النصر، مدحت (2008). تنمية الذكاء العاطفي (الوجداني) مدخل للتميز في العمل والنجاح في الحياة، القاهرة: دار الفجر للنشر والتوزيع.

أبو رياش، حسين، والصابي، عبد الحكيم، وعمور، أميمه، وشريف، سليم (2006). الدافعية والذكاء العاطفي، عمان: دار الفكر للنشر والتوزيع.

باطلي، غنية (2015). الجريمة الإلكترونية- دراسة مقارنة، الجزائر: الدار الجزائرية للنشر والتوزيع.

البشري، محمد الأمين (2005). علم ضحايا الجريمة وتطبيقاته في الدول العربية، الرياض: جامعة نايف للعلوم الأمنية.

البصيصي، صلاح (2008). المعاهدة الدولية والرقابة عليها في ظل الدستور العراقي الجديد، جامعة كربلاء: كلية القانون. ص241-ص255.

البصيصي، صلاح (2015). المعاهدة الدولية والرقابة عليها في ظل الدستور العراقي الجديد، العراق: جامعة كربلاء.

بن شلهوب، محمد (2011). جريمة الإبتزاز - دراسة مقارنة، رسالة ماجستير غير منشورة، السعودية: جامعة الأمام محمد بن سعود الإسلامية.

بنت حجاب، أمينة (2016). تصور مقترح لتنمية الوعي الوقائي لدى الفتيات للوقاية من جرائم الإبتزاز، اطروحة دكتوراه، الرياض: جامعة نايف العربية للعلوم الأمنية.

تشانج، ريتشارد (2002). خطة العاطفة، الرياض: دار جرير للنشر والتوزيع.

جابر عبد الحميد (2003). الذكاءات المتعددة والفهم، القاهرة: دار الفكر العربي.

جروان، فتحي (2012). الذكاء العاطفي والتعلم الاجتماعي والعاطفي، الأردن: دار الفكر.

الجروي، هند بطي (2011). العوامل الاجتماعية والثقافية المؤدية لظاهرة ابتزاز المرأة - دراسة ميدانية في بعض مناطق المملكة العربية السعودية، رسالة ماجستير غير منشورة، الرياض: جامعة الأمام محمد بن سعود الإسلامية.

جريدة الوقائع الفلسطينية (1996). قانون رقم (3) بشأن الاتصالات السلكية واللاسلكية، غزة، بتاريخ 1996/1/18.

جريدة الوقائع الفلسطينية (2017). قانون الجرائم الإلكترونية، عدد 14، رام الله: دار الفتوى والتشريع.

الجعيد، محمد (2011). الذكاء الانفعالي وعلاقته بالتكيف النفسي والاجتماعي لدى طلبة جامعة تبوك في المملكة العربية السعودية، رسالة ماجستير غير منشورة، عمان: جامعة مؤتة.

جهاز الشرطة الفلسطينية (2016). التقرير السنوي لمعدلات الجريمة في الضفة الغربية، فلسطين: إدارة البحوث والتطوير.

الجهاز المركزي للإحصاء الفلسطيني (2014). الإحصاء الفلسطيني ووزارة الاتصالات وتكنولوجيا المعلومات يصدران بيانا صحفيا مشتركا عشية اليوم العالمي لمجتمع المعلومات والذي يصادف السابع عشر من أيار، رام الله.

الجهاز المركزي للإحصاء الفلسطيني (2017). بيان صحفي صادر عن الجهاز المركزي للإحصاء الفلسطيني ووزارة الاتصالات وتكنولوجيا المعلومات بمناسبة اليوم العالمي لمجتمع المعلومات، رام الله.

الجهاز المركزي للإحصاء الفلسطيني(2017). تقرير معالم الفقر في فلسطين، رام الله.

الجوزية ابن قيم، محمد بن أبي بكر (2001). روضة المحبين ونزهة المشتاقين (تحقيق سيد عمران)، القاهرة: دار الحديث.

جولمان، دانييل (2000). الذكاء العاطفي، ترجمة ليلى الجبالي، ط1، الكويت: مكتبة الوطن.

حجازي، عبد الفتاح (2005). الدليل الجنائي والتزوير في جرائم الإنترنت، مصر: دار الكتب القانونية.

الحربي، خالد سليم (2011). ضحايا التهريب البشري من الأطفال، الرياض: جامعة نايف العربية للعلوم الأمنية.

حسن، سالي (2007). الذكاء الوجداني لمعلمات رياض الأطفال، الأزاريطة: دار المعرفة الجامعية.

حسين، سلامة عبد العظيم وحسين، طه عبد العظيم (2006). الذكاء الوجداني للقيادة التربوية، الإسكندرية: دار وفاء لندنيا الطباعة والنشر.

حسين، طه ، وحسين ، سلامة (2006). استراتيجيات إدارة الضغوط التربوية والنفسية، الطبعة الأولى، دار الفكر: عمان.

الحقباتي، رايز (2013). مهارات البحث والتحقيق في الجرائم المعلوماتية- دراسة ميدانية أجريت على ضباط الشرطة بمدينة الرياض، أطروحة دكتوراه غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

حمد، عبد الله (2009). الابتزاز العاطفي، الكويت: منشورات ذات السلاسل.

الحمصي، رولا وبلان، كمال (2010). إدمان الإنترنت عند الشباب وعلاقته بمهارات التواصل الاجتماعيّ دراسة ميدانية على عينة من طلاب جامعة دمشق. مجلة جامعة دمشق للعلوم الإنسانية، ص399- ص417.

حمودة، منتصر (2008). المنظمة الدولية للشرطة الجنائية الإنتربول، الإسكندرية: دار الفكر الجامعي.

الخادمي، نور الدين مختار (2006). الإنترنت والمقاصد الشرعية وقواعدها، ط1، الرياض: مكتبة الرشد.

خطوة، احمد شوقي (2007). شرح الأحكام العامة لقانون العقوبات، القاهرة: دار النهضة العربية.

الخليوي، ممدوح (2014). دور مواقع التواصل الاجتماعيّ في زيادة جريمة الابتزاز ضدّ المرأة من وجهة نظر طالبات الجامعات السعودية، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

الخمشي، سارة (2010). الآثار الاجتماعية السلبية لاستخدام الفتاة في مرحلة المراهقة للإنترنت، مجلة العلوم الإنسانية والاجتماعية، السنة السابعة، العدد45. ص1-44.

الخوالدة، محمود (2004). الذكاء العاطفي- الذكاء الانفعالي، الأردن: دار الشروق للنشر والتوزيع.

دسوقي، محمد سامي (2011). ثورة المعلومات وانعكاسها على الواقع العملي، ندوة الابتزاز المفهوم- الواقع والعلاج ، السعودية: جامعة الملك سعود.

دقيش، أيمن (2010). الابتزاز الجنسي- أسبابه وأساليبه، القاهرة: دار المعارف.

الدليمي، عبد الرزاق محمد (2011). الإعلام الجديد والصحافة الإلكترونية، ط1، عمان: دار وائل للنشر.

ديوان الفتوى والتشريع (2017). قرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية، فلسطين: جريدة الوقائع الفلسطينية.

رعي، أحمد (2015) الابتزاز الإلكتروني، مقابلة- العلاقات العربية والدولية، رام الله: وزارة الداخلية الفلسطينية.

رشوان، حسين عبد الحميد أحمد (1990). الذكاء الأسس النفسية والاجتماعية، الإسكندرية: مركز الإسكندرية للكتاب.

الرفاعي، عبد الرحمن (2012). الذكاء الانفعالي- النظرية والتطبيق في علم النفس الرياضي، الأردن: دار المأمون للنشر والتوزيع.

الرفاعي، عبد الرحمن رجب (2012). الذكاء الانفعالي النظرية والتطبيق في علم النفس الرياضي، الأردن: دار المأمون للنشر والتوزيع.

روبنس، بام وسكوت، جان (2000). الذكاء الوجداني، ترجمة صفاء الأعسر وعلاء الدين الكفافي مترجمون. القاهرة: دار قباء للطباعة والنشر والتوزيع.

ساري، حلمي خضر (2009). ثقافة الإنترنت- دراسة في التواصل الاجتماعي، الأردن: منشورات وزارة الثقافة.

السراني، عبد الله بن سعود بن محمد (2009). فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، الرياض: جامعة نايف العربية للعلوم الأمنية.

السرحاني، محمد (2014). مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت - دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

السعدان، عبد الله حمد والشمري ممدوح محمد (2010). جهود المملكة العربية السعودية في مجال مكافحة الإتجار بالبشر - ورقة علمية قدمت في الملتقى العلمي، الرياض: جامعة نايف العربية للعلوم الأمنية.

السعدون، محمد (2008). الابتزاز أنواعه وأسبابه وأساليب مواجهته، القاهرة: دار النهضة العربية.

سلامي، دلال (2016). الذكاء العاطفي - مدخل نظري، مجلة الدراسات والبحوث الاجتماعية (15)، ص 164 - 179.

السمادوني، إبراهيم (2007). الذكاء الوجداني، الأردن: دار الفكر للنشر والتوزيع.

السويدي، جمال سند (2013). وسائل التواصل الاجتماعي ودورها في التحولات المستقبلية، ط2، الإمارات: مركز الإمارات للدراسات والبحوث الاستراتيجية.

الشاعر، عبد الرحمن بن إبراهيم (2015). مواقع التواصل الاجتماعي والسلوك الإنساني، ط1، عمان: دار الصفاء للنشر.

شقرة، علي خليل (2014). الإعلام الجديد - شبكات التواصل الاجتماعي، ط1، عمان: دار أسامة للنشر والتوزيع.

الشلالدة، محمد، والرعي، عبد الفتاح (2015). الجرائم الإلكترونية في دولة فلسطين المحتلة في ضوء التشريعات الوطنية والدولية- بحث مقدم إلى المؤتمر العلمي الحادي عشر لكلية القانون في جامعة جرش، الأردن: جامعة جرش، بتاريخ 5-7/5-2015.

الشمراي، محمد (2011). ظاهرة الابتزاز في المجتمع السعودي من وجهة نظر العاملين في الضبط الجنائي، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

الشمري، هادي (2011). دور الضحية في حصول الفعل الإجرامي من منظور طلاب الجامعة، رسالة ماجستير غير منشورة. الرياض: جامعة نايف العربية للعلوم الأمنية.

الشميري، فهد بن عبد الرحمن (2010). التربية الإعلامية وكيف نتعامل مع الإعلام، ط1، الرياض: مكتبة الملك فهد الوطنية.

الشويعر، تركي بن صالح بن عبد العزيز (2003). دور التقنيات الحديثة في عملية صنع القرار، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

الصالح، نزار حسين (2011). أثار الابتزاز على الفرد والمجتمع- بحوث ندوة الابتزاز: المفهوم، الأسباب، العلاج، الرياض: مركز باحثات لدراسات المرأة.

الصاوي، محمد منصور (2000). أحكام القانون الدولي في مجال مكافحة الجرائم الدولية للمخدرات، الإسكندرية: دار المطبوعات الجامعية.

طالب، أحسن (2001). الوقاية من الجريمة. بيروت: دار الطليعة.

طالب، أحسن (2007). جرائم الاحتيال والعوامل الاجتماعية والنفسية المهيئة لها، الرياض: جامعة نايف العربية للعلوم الأمنية.

الظاهري، محمد (2017). أثر شبكات التواصل الاجتماعي على الأمن الإنساني، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

الظهواني، حنين (2016). تأثير مواقع التواصل الاجتماعي على المجتمع العربي، المملكة العربية السعودية : جامعة القرى. ص 362-ص 372.

عبابنة، محمود (2009). جرائم الحاسوب وأبعادها الدولية، ط1، عمان: دار الثقافة للنشر والتوزيع.

العبابنة، محمود أحمد (2010). جرائم الحاسوب وأبعادها الدولية، عمان: دار الثقافة للنشر والتوزيع.

عبد الحكيم، مولاي إبراهيم (2015). الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة: الجزائر، العدد 23.

عبد الفتاح، يوسف (2004). الآثار الاجتماعية المترتبة على ارتياد الشباب الجامعي لمقاهي الإنترنت ودور الخدمة الاجتماعية في التعامل معها، مجلة دراسات في الخدمة الاجتماعية والعلوم الإنسانية، مجلد 16 (3)، جامعة حلوان، مصر.

عبد الهادي، حسن محمد (2003). تربويات المخ البشري، عمان: دار الفكر للطباعة والنشر والتوزيع.

عثمان، حباب (2009). الذكاء الوجداني- مفاهيم وتطبيقات، ط1، عمان: دبيونو للطباعة والنشر والتوزيع.

عدس، عبد الرحمن وتوق، محي الدين (2005). المدخل إلى علم النفس، ط6، عمان: دار الفكر للطباعة والنشر والتوزيع.

العلوان، أحمد (2011). الذكاء الانفعالي وعلاقته بالمهارات الاجتماعية وأنماط التعلق لدى طلبة الجامعة في ضوء متغيري التخصص والنوع الاجتماعي للطلاب. المجلة الأردنية في العلوم التربوية . مجلد 7 (2). ص125-144.

- العمر، معن خليل (2009). علم ضحايا الإجرام، الأردن: دار الشروق.
- العمر، معن خليل (2012). جرائم مستحدثة، الأردن: دار وائل للنشر.
- العمر، معن خليل (2015). علم اجتماع الجندر، الأردن: دار الشروق.
- عمران، محمد والعجمي، حمد (2006). أسس علم النفس التربوي - رؤية تربوية إسلامية معاصرة، ط1، الكويت: مكتبة الفلاح للنشر والتوزيع.
- العميرة، محمد (2012). تجريم جرائم ابتزاز النساء - دراسة تأصيلية تطبيقية، رسالة ماجستير غير منشورة. الرياض: جامعة نايف العربية للعلوم الأمنية.
- العميري، محمد بن عبد الله (2004). موقف الإسلام من الإرهاب، الرياض: جامعة نايف العربية للعلوم الأمنية.
- العنزي، خالد عسكر (2010). الابتزاز تعريفه وأنوعه وأسبابه وعلاجه، رسالة ماجستير غير منشورة: السعودية: جامعة أم القرى.
- عودة، عبد القادر (2008). التشريع الجنائي الإسلامي مقارنا بالقانون الوضعي، بيروت: دار الكتاب العربي.
- عوض، السيد (2004). الجريمة في مجتمع متغير، الإسكندرية: المكتبة المصرية.
- عوض، محمد محي الدين (2004). الدعوة الجنائية ودور المدعي العام فيها، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.
- العيسى، وفاء (2011). جنين الإبتزاز - بحوث ندوة الإبتزاز: المفهوم والأسباب العلاج، الرياض: مركز باحثات لدارسات المرأة.

كاتب، سعود صالح (2011). الإعلام الجديد وقضايا المجتمع - التحديات والفرص، المؤتمر العالمي الثاني للإعلام الإسلامي، رابطة العالم الإسلامي، جدة ، السعودية.

كردي، سميرة (2009). الاكتئاب والذكاء الانفعالي لدى عينة من مدمنات الإنترنت: دراسة وصفية مقارنة، مجلة دراسات نفسية. المجلد 19 (1). ص121-166

الكعبي، محمد (2009). الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الإنترنت، القاهرة: دار النهضة العربية.

محمد، علاء (2009) الذكاء الوجداني والتفكير الابتكاري عند الأطفال، عمان: دار الفكر للنشر والتوزيع.

محمود، سليمان ومطر عبد الفتاح (2002). أساليب المعاملة الوالدية وعلاقتها بالذكاء الانفعالي لدى الأبناء، مجلة التربية، العدد 111.

المحمود، محمد(2014). المسؤولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة- دراسة تأصيلية تطبيقية، أطروحة دكتوراه غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

مسعود، جبران(1992). الرائد معجم لغوي عصري، ط7، بيروت: دار العلم للملايين.

المطيري، سامي مرزوق(2015). المسؤولية الجنائية عن الابتزاز الإلكتروني في النظام السعودي، الرياض: جامعة نايف العربية للعلوم الأمنية.

المليجي، حلمي (1985). علم النفس المعاصر، ط1، الإسكندرية: دار المعرفة الجامعية.

المناعسة، أسامة والزعبي، جلال (2014). جرائم تقنية المعلومات الإلكترونية- دراسة مقارنة وفقا لقانون جرائم أنظمة المعلومات رقم (30) لسنة (2010) والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2012، عمان: دار الثقافة للنشر والتوزيع.

المنصور، محمد(2012). تأثير شبكات التواصل الاجتماعي على الجمهور المتلقين - دراسة مقارنة للمواقع الاجتماعية والمواقع الإلكترونية، رسالة ماجستير غير منشورة، الدنمارك: الأكاديمية العربية.

موسى، رشاد(2012). الذكاء العاطفي وتنميته في مرحلة الطفولة والمراهقة، ط1، القاهرة: عالم الكتب.

ناصر، الرئيس وآخرون(2003). مشروع قانون العقوبات الفلسطيني - أوارق عمل - سلسلة مشروع تطوير القوانين (17)، رام الله: الهيئة المستقلة لحقوق المواطن.

نصر، إبراهيم(2015). البرنامج التمهيدي للتدريب على استخدام الحاسوب والإنترنت - مقدمة للإنترنت، جامعة سرها: مكتب التدريب.

النصر، تركي(2017). التحقيق في جرمي التحرش والابتزاز عبر الشبكات الإلكترونية - دراسة تطبيقية على هيئة التحقيق والادعاء العام بالمنطقة الشرقية، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

النفيعي، مزيد(2002). مقاهي الإنترنت والانحراف إلى الجريمة بين مرتاديهها، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية.

الهيومل، محمد(2009). جرائم ابتزاز الفتيات وطرق اكتشافها والتحقيق فيها، الرياض: جامعة نايف العربية للعلوم الأمنية.

الهيبي، محمد حماد مهرج(2005). جرائم الحاسب ماهيتها - موضوعها - أهم صورها - والصعوبات التي تواجهها، عمان: دار المناهج للنشر والتوزيع.

الوشلي، أمة الرزاق أحمد(2003) الصحة النفسية لدى طلبة جامعة صنعاء وعلاقتها بالضغط النفسية، أطروحة دكتوراه غير منشورة، السودان: جامعة الخرطوم.

ثانياً: المصادر والمراجع الأجنبية:

Bar-On, Rauven (2005). The impact of emotional intelligence on subjective well-being, **Personality in education**, vol. 23 (2) 41- 62.

Bar-On, Rauven, & Parker, James (2000). **Emotional Quotient Inventory: Youth Version (EQ-i:YV): Technical manual**. Toronto, Canada: Multi-Health Systems.

Catalan, Maria, & Zych, Izabela, & Ruiz, Rosaria, & Llorent, Vicente (2017) . Victimization through bullying and cyberbullying: Emotional intelligence, severity of victimization and technology use in different types of victims. Universidad de Córdoba. **Psicothema**. 30(2):183-188. doi: 10.7334/psicothema2017.313.

Clark, Robert (1972).**Reference Group Theory and Delinquency**, New York: Behavioral Publications.

Cohen, Lawrence & Felson, Marcus (1979) . Social change and crime rate trends- A routine activities approach, **American Sociological Review** 44, 588-608.

Cooper, Robert, & Sawaf, Ayman (1997). **Executive EQ: emotional intelligence in leadership and azganictions**. New york: the Berkleypublishing Group.

Council of Europe(1989)- Explanatory Report to the Convention on Cybercrime , (ETS No.185) Introduction, No. 111, The Convention , p.3. doi: 10.4103/0972-6748.160934.

Donnerstein, Edward, & Linz, Daniel (1995) .**The Media. In James Q. Wilson and Joan Petersillia (eds)**, Crime. San Francisco: ICS Press.

Elipe, Paz and Merchán, Joaquín and Ruiz, Rosario and Casas, José.(2015). **Perceived emotional intelligence as a moderator variable between cybervictimization and its emotional impact**. *Frontiers in Psychology*. published: 23 April 2015 .doi: 10.3389/fpsyg.2015.00486.

Hampson, Kathy (2012). **The role of emotional intelligence in the criminal activity of young people involved with the Leeds Youth Offending Service**, Submitted in accordance with the requirements for the degree of PhD. University of Leeds, School of Law.

Kornhauser, Ruth Roser (1978) .**Social Sources of Delinquency**. Chicago: University of Chicago Press.

Leonhardt, Marion ,& Matthews, Stephen ,& Meaney, Michael ,& Walkera, Claire (2007). Psychological stressors as a model of maternal adversity: Diurnal modulation

of corticosterone responses and changes in maternal behavior. **Hormones and Behavior** Volume 51, Issue 1, January 2007, Pages 77-88.

Mayer, David, & Salovey, Peter (1990). **Emotional intelligence imagination cognition and personality**, 9(3).

Mayer, David, & Salovey, Peter (1997). **What is Emotional Intelligence?, In peter, Salovey, & David, Sluyter , Emotional Development and Emotional Intelligence: Educational Implications**, New York: Basic Books, 3-34.

Mayer, John, & Caruso, David, & Salovey, Peter (2000). Selecting a measure of emotional intelligence: The case of ability scales. In R. Bar-On, & J. D. A Parker (Eds.), *Handbook of emotional intelligence* (pp. 320-342). San Francisco: Jossey-Bass.

Megreya, Ahmad(2014). Emotional Intelligence and Criminal Behavior, **JOURNAL OF FORENSIC SCIENCES**. J Forensic Sci, 2014 doi: 10.1111/1556-4029.12625.

Ojedokun , Oluyinkam, & Idemudia, Erhabor (2013). The Moderating Role of Emotional Intelligence between PEN Personality Factors and Cyberbullying in a Student Population. **Life Science Journal** 2013;10(3).

Sharma, Neelu, & Prakash, Om, & Suprakash, Chaudhury, & Singh , Amool (2015). The relation between emotional intelligence and criminal behavior: A study among convicted criminals, **Ind Psychiatry J**. 2015 Jan-Jun; 24(1): 54–58.

UNODC (2013). **Comprehensive Study on Cybercrime**, United Nations Office on Drugs and Crime, United Nations.

Wall, David (2007). **Cybercrime: The Transformation of Crime in the Information Age** , Cambridge, UK, 288 pages.

Wang, Caikang (2002). Emotional intelligence- general self-efficacy and coping style of Juvenile delinquents, **Chinese Mental Health Journal**, Vol. 16 (8) 565-567.

ثالثاً: مصادر المواقع الإلكترونية:

Number of Internet Users (2014) Internet Live stats, www.inernetlivestats internet-users, 22-7-2017, 00:02 PM.

البار، محمد علي (1987). الابتزاز الجنسي للمرأة العاملة في الغرب، المغرب: مجلة الفرقان. عدد10، للمزيد انظر/ي الرابط الإلكتروني:

<https://www.cia.gov/library/abbottabad-compound> . 10-09-2019, 12:52 PM

يماني، أماني (2017). 978 مليون ضحية للجرائم الإلكترونية في 20 بلداً، للمزيد انظر/ي الرابط الإلكتروني:

<https://makkahnewspaper.com/article/1096455/%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85/978-%D9%85%D9%84%D9%8A%D9%88%D9%86-%D8%B6%D8%AD%D9%8A%D8%A9-%D9%84%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%8A-20-%D8%A8%D9%84%D8%AF%D8%A7, 23-11-2019, 21-11-2019, 21:02 PM>.

جهاز الشرطة الفلسطينية (2019). تقرير من إدارة وحدة العلاقات العامة والإعلام بالشرطة، للمزيد انظر/ي الرابط الإلكتروني:

<http://www.palpolice.ps/ar/content/728362.html> ,01-09-2019,15:30 PM.

جهاز الشرطة الفلسطينية (2019). الجريمة الإلكترونية جريمة العصر-دراسات وإحصائيات ، للمزيد انظر/ي الرابط الإلكتروني:

<http://www.palpolice.ps/ar/content/726833.html> , 22-10-2019, 20:55 PM.

النعامي، صالح (2007). الوحدة (8200) ذراع التجسس الإلكتروني لإسرائيل، للمزيد انظر/ي الرابط الإلكتروني:

<https://www.voltairenet.org/article146534.html> ,13-12-2018, 21: 51 PM.

الأوجلي، سالم (2006). التحقيق في جرائم الكمبيوتر والإنترنت، للمزيد انظر/ ي الرابط الإلكتروني:

<http://afaitouri.maktoobblog.com/1624946/>, 30-06-2017, 20: 48 PM.

الغافري، حسين (2014). جهود سلطنة عمان في مواجهة الجرائم المتعلقة بشبكة الإنترنت، للمزيد انظر/ ي الرابط الإلكتروني:

<http://hussain-alghafri.blogspot.com/>, 06-09-2017, 12: 52 AM.

غفري، محمد (2015). محاولات خفية علنية لأجهزة الشبكات تستهدف إسقاط غزة عبر موقع الفيس بوك، للمزيد انظر/ ي الرابط الإلكتروني:

<https://www.alhadath.ps/article/23713/%D9%81%D9%8A-%D8%A7%D9%84%D8%B9%D8%AF%D8%AF-48-%D9%85%D8%AD%D8%A7%D9%88%D9%84%D8%A7%D8%AA-%D8%AE%D9%81%D9%8A%D8%A9-%D8%B9%D9%84%D9%86%D9%8A%D8%A9-%D9%84%D8%A3%D8%AC%D9%87%D8%B2%D8%A9-%D8%A7%D9%84%D8%B4%D8%A7%D8%A8%D8%A7%D9%83-%D8%AA%D8%B3%D8%AA%D9%87%D8%AF%D9%81-%D8%A5%D8%B3%D9%82%D8%A7%D8%B7-%D8%B4%D8%A8%D8%A7%D8%A8-%D8%BA%D8%B2%D8%A9-%D8%B9%D8%A8%D8%B1-%D8%A7%D9%84%D9%81%D9%8A%D8%B3-%D8%A8%D9%88%D9%83> , 20-7-2018, 11: 50 AM.

الهيئة المستقلة لحقوق الإنسان (2018). الهيئة ترحب بصدور القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية-الملاحظات والتحفظات، للمزيد انظر/ ي الرابط الإلكتروني:

<https://ichr.ps/ar/1/26/2389/%D8%A7%D9%84%D9%87%D9%8A%D8%A6%D8%A9-%D8%AA%D8%B1%D8%AD%D8%A8-%D8%A8%D8%B5%D8%AF%D9%88%D8%B1-%D8%A7%D9%84%D9%82%D8%B1%D8%A7%D8%B1->

[%D8%A8%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%B1%D9%82%D9%85-\(10\)-%D9%84%D8%B3%D9%86%D8%A9-2018-%D8%A8%D8%B4%D8%A3%D9%86-%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D8%AA%D9%82%D8%AF%D9%85-%D9%85%D8%AC%D9%85%D9%88%D8%B9%D8%A9-%D9%85%D9%86-%D8%A7%D9%84%D9%85%D9%84%D8%A7%D8%AD%D8%B8%D8%A7%D8%AA-%D9%88%D8%A7%D9%84%D8%AA%D8%AD%D9%81%D8%B8%D8%A7%D8%AA.htm, 12-04-2018, 19:48 PM.](#)

الشامي، عبد الخالق (2010). جرائم الكمبيوتر والإنترنت في التشريع الفلسطيني، للمزيد انظر / ي الرابط الإلكتروني:

<https://pulpit.alwatanvoice.com/articles/2010/05/02/196865.html>, 13-9-2018, 09:45 AM.

مركز معلومات G-8 (2011). جهود مجموعة الدول الثمانية G-8 لمكافحة الجريمة الإلكترونية، للمزيد انظر / ي الرابط الإلكتروني:

<https://www.hsdl.org/?abstract&did=475747> , 06-11-2017, 19: 34PM.

باوزير، وفاء (2016). نظرية ديسك، للمزيد انظر / ي الرابط الإلكتروني:

<https://wafabawazeer.wordpress.com/tag/%D9%86%D8%B8%D8%B1%D9%8A%D8%A9-disc/> , 02-06-2019, 08: 28 AM.

عتمه، رعدة (2019). الجرائم الإلكترونية في فلسطين - تهديد وابتزاز ومحاولات انتحار، للمزيد انظر / ي الرابط الإلكتروني:

<https://www.independentarabia.com/node/46931/%D8%AA%D8%AD%D9%82%D9%8A%D9%82%D8%A7%D8%AA-%D9%88%D9%85%D8%B7%D9%88%D9%84%D8%A7%D8%AA/%D8%A7%D9%84%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%81%D9%8A-%D9%81%D9%84%D8%B3%D8%B7%D9%8A%D9%86%E2%80%A6-%D8%AA%D9%87%D8%AF%D9%8A%D8%AF-%D9%88%D8%A7%D8%A8%D8%AA%D8%B2%D8%A7%D8%B2-%D9%88%D9%85%D8%AD%D8%A7%D9%88%D9%84%D8%A7%D8%AA-%D8%A7%D9%86%D8%AA%D8%AD%D8%A7%D8%B1%23-11-2019, 19:27 PM.>

كرسوع، هنادي (2016). تحقيق الابتزاز الإلكتروني بين الواقع والشرع والقانون، للمزيد انظر/ ي الرابط الإلكتروني:

<http://www.police.ps/ar/include/plugins/news/news.php?action=s&id=7969,>
22-09-2019, 19:23 PM.

ليدك، ليندساي (2019). 100+ إحصاءات الإنترنت والحقائق لـ2019، للمزيد انظر/ ي الرابط الإلكتروني:

<https://www.websitehostingrating.com/ar/internet-statistics-facts/,10-11-2019, 19:21 PM.>

قائمة الملاحق

ملحق (1) الاستبانة في صورتها الأولى:



جامعة القدس

عمادة الدراسات العليا

ماجستير الخدمة الاجتماعية

إخوتي الضحايا

تحية طيبة وبعد...

تقوم الباحثة بإجراء دراسة بعنوان: "الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية"، ذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في الخدمة الاجتماعية. أرجو التكرم بالإجابة عن فقرات الإستبانة ووضع إشارة (X) أمام العبارة التي تتفق ووجهة نظرك. شاكره لكم جهودكم وأمانتكم وحرصكم على إنجاز هذه الدراسة، علماً أن إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار، ولن تستخدم إلا لأغراض البحث العلمي فقط.

مع خالص شكري لحسن تعاونكم

الباحثة: نورهان عابدين

إشراف: د. وفاء الخطيب

أولاً: البيانات الأولية:

ضع دائرة حول الصفة التي تنطبق على حالتك:

1. الجنس:

أ. ذكر. ب. أنثى .

2. المستوى التعليمي :

أ. أمي. ب. (إعدادي- ثانوي) ج. دبلوم . د. بكالوريوس. هـ. دكتوراه.

3. مكان السكن :

أ. قرية. ب. مخيم . ج. مدينة .

4. العمر :

أ. 18 - 30 سنة. ب. 31-43 سنة. ج. 44 - 56 سنة. د. 57 فأكثر.

5. مستوى الدخل :

أ. 500-1000 شيكل . ب. 1100-1600 شيكل. ج. 1700-2200 شيكل.

د. 2300 شيكل فأكثر.

6. الحالة الاجتماعية :

أ. أعزب . ب. متزوج . ج. مطلق. د. أرمل .

7. علاقتك مع الآخرين:

أ. جيدة جداً. ب. جيدة. ج. جيدة أحياناً.

8. مدى استخدامك لشبكات مواقع التواصل الاجتماعي:

أ. كثيراً. ب. قليلاً. ج. نادراً.

9. عدد ساعات استخدامك لمواقع التواصل الاجتماعي في اليوم:

أ. ساعة واحدة فأقل. ب. أقل من ساعتين. ج. ساعتين. د. أقل من ثلاث ساعات.

هـ. 3 ساعات فأكثر.

ثانياً: مقياس الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني.

يرجى وضع إشارة (صح) في المربع الذي يتفق ووجهة نظرك أمام كل فقرة من الفقرات التي تمثل

الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني

الرقم	الفقرة	بدرجة كبيرة جدا	بدرجة كبيرة	بدرجة متوسطة	بدرجة ضعيفة	بدرجة ضعيفة جدا
		تصلح	لا تصلح	اقترح التعديل		
أولاً: مستوى الذكاء العاطفي لدى ضحايا جريمة الابتزاز الإلكتروني						
1	أستطيع أن أصف مشاعري بسهولة.					
2	أعرف كيف أقضي وقتنا طيباً.					
3	أنا لست سعيداً جداً.					
4	أنا مدرك لعواطفني التي أمر بها.					
5	أحب أن أشارك الآخرين عواطفني.					
6	أستطيع بسهولة استخدام طرق متعددة لحل مشكلاتي.					
7	أستطيع ان اخبر الآخرين بما أشعر بسهولة.					
8	أضايق بسهولة.					
9	أتحكم في انفعالاتي.					
10	عندما أغضب أتصرف بدون تفكير.					
11	يصعب علي التحدث عن مشاعري العميقة .					
12	يعجبني مظهري.					
13	يعجبني جسدي.					

14	عندما أغضب من أحد، أبقى غاضبا مدى طويلة.		
15	أشعر بالاستياء عند إيذاء مشاعر الآخرين.		
16	أعتقد أنني الأفضل في كل شيء أقوم به.		
17	أنا سريع الغضب.		
18	عندما أفرح أفقد السيطرة على نفسي.		
19	أتغلب على مشاكل دون انفعال.		
20	يصعب على وصف ما أشعر به.		
21	أستطيع تميز عواطفى السلبية من الإيجابية.		
22	أستطيع أن أحس بآلام الآخرين.		
23	أستطيع ان أحقق السعادة بنفسى.		
24	التزم الهدوء عند انفعال الآخرين.		
25	قدرتى لتحقيق إنجازات جديدة ضعيفة.		

ثانياً: الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية

26	علاقة عاطفية بين المبتز والضحية لتحقيق أهدافه.		
27	إرسال معلومات وبيانات وهمية على إنها تخص مبتز لكسب ثقة الضحية.		
28	اختراق البريد الإلكتروني أو الحساب على مواقع التواصل الاجتماعي للحصول على المعلومات والبيانات الخاصة بالضحية.		
29	قيام المبتز بانتحال شخصيات أخرى وإخفاء شخصيته للوصول للضحية المناسبة .		

30	ابتزاز وتهديد الضحية بنشر الصور والمحادثات على مواقع التواصل الاجتماعي حتى يستجيب له الضحية.
31	استغلال المبتز حسابات الضحية على مواقع التواصل الاجتماعي من خلال المعلومات التي ينشرها عن حياته الخاصة .
32	استغلال المبتز لقدرته العالية ومهارته في استخدام الشبكة العنكبوتية في جريمة الابتزاز الإلكتروني، بالإضافة إلى غياب الحراسة .
33	استخدام أسلوب التهديد بالفضيحة للإيقاع بالضحية .
34	وعود الضحية بالحصول على علاقة عاطفية يطمح إليها .
35	إرسال المبتز لروابط ومواقع الكترونية تؤدي إلى اختراق حسابات وجهاز الضحية مما يؤدي إلى وصول المبتز لكافة المعلومات والبيانات التي يحتاجها لابتزاز الضحية.
36	اختيار الضحية المناسب الذي يتمتع بتدني تقدير لذاته ولا يثق بنفسه.

ثالثاً: الإجراءات المتبعة من وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة للتعامل مع ضحايا جرائم الابتزاز الإلكتروني.

37	متابعة البلاغات باهتمام بالغ وتتبع المبتز .
38	إتباع قانون الجرائم الإلكترونية في فرض العقوبة المناسبة على المبتز ذلك لحماية الضحية.
39	تساند وحدة الجرائم الإلكترونية ووحدة حماية الأسرة ضحايا جريمة الابتزاز الإلكتروني.

			40	التكتم والمحافظة على سرية وخصوصية الضحية خوفا من تبعيات جريمة الابتزاز الإلكتروني التي حصلت له.
			41	تستخدم وحدة الجرائم الإلكترونية الضحية كأداة للمساعدة في القبض على المبتز.
			42	يحق لوحدة الجرائم الإلكترونية القبض على المبتز ومصادرة الأدوات التي استخدمتها في جريمته.
			43	حماية الضحية حين لجوئه لوحدة جرائم الإلكترونية وتحويله إلى وحدة حماية الأسرة إذا لزم الأمر.
			44	إيقاف جريمة الابتزاز الإلكتروني .
			45	التدخل في سير جريمة الابتزاز الإلكتروني للقبض على المبتز متلبسا أثناء ارتكابه جريمة الابتزاز الإلكتروني.
			46	تفعيل دور المرشد الاجتماعي والنفسي في التعامل مع الضحية.
			47	يتوافر رقم موحد للتبليغ عن جرائم الابتزاز الإلكتروني.
			48	التواصل مع المجرم لمعرفة دوافعه ومحاولة إيقاف الجريمة.
			49	اللجوء ببعض الأحيان إلى الجهات العشائرية لحل جريمة الابتزاز الإلكتروني بطرق ودية.
			50	تحديد نوعية الابتزاز ليتم تحديد الآلية المناسبة للتعامل معه.
			51	تحديد المعلومات والبيانات التي تم الاستلاء عليها لابتزاز الضحية .
			52	اعتماد التسجيلات الصوتية والمحادثات لمواجهة

			المبتز والتي تتضمن تهديدات المبتز للضحية.	
53			إعطاء الضحية تعليمات وتوجيهات للتعاون في القبض على المبتز .	
54			اختراق جهاز المبتز وتدمير كافة البيانات والمعلومات التي يمتلكها عن الضحية ويبتز بها.	
55			تقوم وحدة الجرائم الإلكترونية بحملات توعية بخطورة الابتزاز الإلكتروني وآثاره.	
56			دور وحدة الجرائم الإلكترونية ليس القبض على المبتز فقط وإنما تعمل على وضع خطط لمعالجتها.	
57			جميع إجراءات وحدة الجرائم الإلكترونية تتم سرية تامة وذلك للحفاظ على سمعة الضحية.	
رابعاً: الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.				
58			انتشار الفحاشة عند حدوث ابتزاز الكتروني جنسي بين الضحايا والمبتزين.	
59			تفكك اسري وحدث حالات طلاق في بعض الأسر.	
60			سلب الموارد المادية للضحية في حالة التعرض لابتزاز الكتروني مادي.	
61			حدث خلافات عائلية عند معرفة المبتز والضحية لبعضهم البعض.	
62			قد يلجأ ببعض الأحيان أهل الضحية الى قتله بعد تعرضه للابتزاز الإلكتروني خوفاً من الفضيحة والعار.	
63			زيادة معدل جرائم الابتزاز الإلكتروني بشكل عام.	
64			في بعض الحالات قد تؤدي جريمة الابتزاز الإلكتروني	

			إلى تهديد الأمن العام تبعا لانتماء الضحية .
65			تراجع قوة القيم والأعراف والتقاليد لردع السلوك المنحرف في المجتمع.
66			قد يلجأ المبتز إلى الضغط على الضحية لارتكاب مخالفات أخلاقية وقانونية.
67			الابتعاد عن الدين وانتشار الأفعال الغير سوية بين المبتزين.
68			التلاعب بمشاعر الضحية عند ارتكاب المبتز جريمة ابتزاز الكتروني عاطفي.
69			تراجع ثقة الضحية بنفسه .
70			بعض جرائم الابتزاز الإلكتروني لا تكون مختصره على حدود الدولة بل يتعدى ذلك إلى دول أخرى قد ينتج عنها خلافات سياسية بين عدة دول.
71			قد يلجأ الضحية إلى الانتحار للتخلص من المبتز .
72			انعزال الضحية عن البيئة المحيطة.
73			تراجع دافعية الضحية للحياة ورغبته بالموت لإنهاء جريمة الابتزاز الواقعة عليه.
74			تدني الذكاء العاطفي عما قبل الجريمة التي وقعت عليه.
75			نتيجة حالة الكتمان التي يمر بها ضحية جريمة الابتزاز الإلكتروني من المرجح حدوث أمراض سيكوسيدية له.
76			يصبح مزاج الضحية حاد.

			77	تدني الكفاءة الشخصية لدى الضحية في حلّ مشاكله أو التفكير السوي.
--	--	--	----	--

مقترحات للتعديلات:

.....

.....

.....

.....

مع خالص الاحترام والتقدير

ملحق (2) الاستبانة في صورتها النهائية:



جامعة القدس

عمادة الدراسات العليا

ماجستير الخدمة الاجتماعية

إخواني/أخواتي الأعزاء

تحية طيبة وبعد ...

تقوم الطالبة بإجراء دراسة بعنوان: "الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا في الضفة الغربية"، ذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في الخدمة الاجتماعية. الرجاء التكرم بالإجابة عن فقرات الاستبانة ووضع إشارة (V) أمام العبارة التي تتفق ووجهة نظركم. شاكرة لكم جهودكم وأمانتكم وحرصكم على إنجاز هذه الدراسة، علماً أن إجاباتكم ستكون سرية ولا تشكل أي نوع من الاختبار، ولن تستخدم إلا لأغراض البحث العلمي فقط.

مع خالص شكري لحسن تعاونكم

الطالبة: نورهان عابدين

المشرف : د. وفاء الخطيب

القسم الأول: البيانات الشخصية:

يرجى وضع إشارة (√) على الصفة التي تنطبق على حالتك:

1. الجنس:

- ذكر (1)
 أنثى (2)

2. المستوى التعليمي:

- (1) لا يقرأ ولا يكتب.
 (2) ابتدائي.
 (3) إعدادي.
 (4) ثانوي .
 (5) دبلوم.
 (6) بكالوريوس.
 (7) دراسات عليا فما أعلى.

3. مكان السكن:

- (1) قرية.
 (2) مخيم .
 (3) مدينة .
 (4) غير ذلك حدد/ي:

4. العمر:

- (1) من 18- أقل من 23 سنة.
 (2) من 23- أقل من 28 سنة.
 (3) من 28- أقل من 33 سنة.
 (4) من 33- أقل من 38 سنة.
 (5) من 38- أقل من 43 سنة.
 (6) 43 فما فوق.

5. الوظيفة:

- (1) يعمل/ تعمل.
- (2) لا يعمل/ لا تعمل.
- (3) طالب/ طالبة

6. مستوى الدخل:

- (1) من 1450- أقل من 2450 شيكل.
- (2) من 2450- أقل من 3450 شيكل.
- (3) من 3450 - 4450 شيكل.
- (4) 4450 شيكل فأكثر.

7. الحالة الاجتماعية:

- (1) أعزب/ عزباء .
- (2) متزوج/ متزوجة.
- (3) مطلق/ مطلقة.
- (4) أرمل/ أرملة .
- (5) معلق/ معلقة.

8. معدل استخدامك لمواقع التواصل الاجتماعي في اليوم حدد/ي: ساعة.

القسم الثاني: مجالات الدراسة

الجزء الأول: مقياس الذكاء العاطفي

يرجى وضع إشارة (✓) في المربع الذي يتفق ووجهة نظركم أمام كلّ فقرة من الفقرات التالية:

الرقم	الفقرات	أوافق بشدة	أوافق	محايد	أعارض	أعارض بشدة
أولاً: مستوى الذكاء العاطفي لدى ضحايا جريمة الابتزاز الإلكتروني						
1.	أحسن الظن بالآخرين					
2.	أعبر عن مشاعري بدقة					
3.	إذا تعرضت لمحنة ما أخفف عنها بنفسني					
4.	استطيع أن أحدد العديد من الأشياء التي (اشمئز، أقرف) منها					
5.	أدرك مشاعري كلما تغيرت					
6.	لديّ مشاعر سلبية					
7.	ليس لدي الشجاعة لأرد الإهانة بمثلها					
8.	أجد صعوبة في التعبير عن أفكاري					
9.	أتردد في توجيه اللوم لشخص يسئ للآخرين					
10.	أنا جدير باحترام الآخرين					
11.	أنا جدير بحب الآخرين					
12.	عادة استطيع أن افعل ما احتاجه عاطفياً بإرادتي					
13.	أعتقد أنني قذوة صالحة					
14.	أنا أقل أهمية من الآخرين					

					15. في المواقف الاجتماعية عندي أفكار مهمة أقولها
					16. أتعامل مع الآخرين باحترام متبادل
					17. أتقبل الواقع كما هو (حلوه، مره)
					18. أنا فاشل
					19. أستطيع احتواء مشاعر الإجهاد التي تعوق أدائي لمهامتي
					20. أجد صعوبة في أن أبدا أنشطة جديدة بمفردتي
					21. أفضل أن يتخذ الآخرين قراراتي
					22. أوافق أو أرفض حسب رأي المجموعة
					23. أتجنب إيذاء مشاعر الآخرين
					24. أنا سعيد في حياتي
					25. أفرح لفرح الناس
					26. أحزن لحزن الناس
					27. أشعر بالفشل في علاقاتي الاجتماعية

الرقم	الفقرات	أوافق بشدة	أوافق	محايد	أعارض	أعارض بشدة
28.	غيابي لفترة طويلة لا يشعر به من حولي					
29.	لدي قناعة بأن علاقاتي مع الآخرين مؤقتة					
30.	إذا تعارضت مصلحتي مع المصلحة العامة أنتازل عن مصلحتي					
31.	أجد صعوبة في التوصل لحل المشكلات التي تواجهني					
32.	أتجنب انفعالات "القلق، الغضب، الخوف" في موقف حلّ المشكلة					
33.	أشعر بان الواقع (زائف، وخداع)					
34.	انا مندفع وراء "أحلامي، خيالاتي"					
35.	انطباعي الأول عن الأشخاص لا يتغير					
36.	كلما ازدادت همومي، أنام لساعات طويلة					
37.	أتعامل مع الشدائد بعصبية					
38.	كثير من تصرفاتي تغضب الآخرين					
39.	أثورط في مجازفات جديدة					
40.	روحي المعنوية مرتفعة					
41.	تحاصرني الهموم من كلّ اتجاه					

الجزء الثاني: واقع ممارسة جرائم الابتزاز الإلكتروني

أولاً: الوسائل المستخدمة للإيقاع بضحايا جرائم الابتزاز الإلكتروني في الضفة الغربية					
					42. العلاقات العاطفية
					43. استدراج الضحية
					44. اختراق مواقع التواصل الاجتماعي الخاصة بالضحية للحصول على معلومات خاصة بالضحية
					45. قيام المبتز بانتحال شخصيات أخرى للوصول إلى الضحية
					46. ابتزاز الضحية بنشر "الصور، المحادثات" الخاصة به على مواقع التواصل الاجتماعي
					47. استغلال المبتز "لقدراته، مهاراته" العالية في استخدام الشبكة العنكبوتية للقيام في جريمة الابتزاز الإلكتروني
					48. إرسال المبتز روابط تؤدي إلى اختراق حسابات الضحية للوصول إلى المعلومات الخاصة بها
					49. وعود الضحية بالحصول على علاقة عاطفية يطمح إليها
					50. اختيار الضحية المناسبة التي تتمتع بتدني تقدير الذات
					51. استغلال المبتز غياب الرقابة على مواقع التواصل الاجتماعي
					52. الدخول إلى حساب الضحية من خلال الهكر
					53. التسلسل الغير مشروع لبيانات المحفوظة على جهاز الضحية الذي تمّ (تصليحه، ضياعه)
					54. استخدام المواقع الإباحية كوسيلة لأغراء الضحية
					55. عروض الزواج الوهمية

					56. إرسال المبتز معلومات خاصة به لكسب ثقة الضحية
					58. اختراق مواقع التواصل الاجتماعي الخاصة بالضحية للحصول على "معلومات، بيانات" خاصة بالضحية
					59. قيام المبتز بانتحال شخصيات أخرى للوصول إلى الضحية المناسبة
ثانياً: أهم الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني من وجهة نظرك/ي.					
					60. ارتفاع نسبة البطالة
					61. ارتفاع نسبة الثراء لدى طبقة معينة في المجتمع
					62. ضغوط الحياة العامة (الاقتصادية، الاجتماعية، السياسية، الصحية)
					63. ضعف تنفيذ القوانين الخاصة بالجرائم الإلكترونية
					64. سرعة تنفيذ الجريمة الإلكترونية
					65. التحدي بين الشباب
					66. استخدم الاحتلال في العديد من الأحيان الابتزاز الإلكتروني وسيلة لتحقيق مآربه
					67. ضعف الوازع الديني
					68. التفكك الأسري
					69. انعدام الرقابة "الذاتية، المجتمعية"
					70. استفزاز الضحية للمبتز
					71. نمط الحياة التي يتعامل بها الفرد مع الآخرين
					72. الاختلاط بأصدقاء السوء

					73. عدم وجود رقابة حكومية على مواقع التواصل الاجتماعي
					74. ارتفاع نسبة البطالة
					75. الخوف المجتمعي
					76. الخوف الذاتي
					77. عدم الثقة بالوحدة
					78. عدم الثقة بالقضاء
					79. عدم الثقة بالأشخاص
					80. عدم القدرة على اختيار جهة الدعم
ثالثاً: الإجراءات المتبعة من وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في جهاز الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة في التعامل مع ضحايا جرائم الابتزاز الإلكتروني					
					81. إتباع قانون الجرائم الإلكترونية في فرض العقوبة المناسبة على المبتز
					82. مساندة ضحايا جريمة الابتزاز الإلكتروني
					83. استخدام الضحية كأداة للمساعدة في القبض على المبتز
					84. التدخل في سير جريمة الابتزاز الإلكتروني للقبض على المبتز متلبساً أثناء ارتكابه جريمة الابتزاز الإلكتروني
					85. تفعيل دور المرشد "الاجتماعي، النفسي" في التعامل مع الضحية
					86. توفير رقم موحد للتبليغ عن جرائم الابتزاز الإلكتروني
					87. اللجوء إلى الجهات العشائرية لحل جريمة الابتزاز الإلكتروني بطرق ودية

					89. تحديد نوعية الابتزاز ليتم تحديد الآلية المناسبة للتعامل معه
					90. مواجهة المُبتز بمحادثات التهديد التي قام بها
					91. اختراق جهاز المبتز بهدف تدمير كافة (البيانات، المعلومات) التي يبتز بها الضحية
					92. تقوم بحملات توعية عن خطورة الابتزاز الإلكتروني
					93. تعمل على وضع خطط لمعالجة جرائم الابتزاز الإلكتروني
					94. التأكيد على الضحية بعدم التعاون مع المبتز
					95. تحويل الضحية إلى وحدة حماية الأسرة إذا لزم الأمر
					96. جميع إجراءاتها تتم بسرية تامة، ذلك للحفاظ على سمعة الضحية
					97. تعزيز (التعاون، التنسيق) مع المؤسسات (الدولية، المحلية) المعنية بمكافحة الجرائم الإلكترونية
رابعا: الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا					
					98. انتشار الانحراف بين الضحايا والمبتزين
					99. التفكك اسري
					100. الطلاق
					101. سلب الموارد المادية للضحية
					102. حدوث خلافات عائلية عند معرفة المبتز والضحية لبعضهم البعض
					103. تعرض الضحية للقتل من قبل عائلته خوفا من الفضيحة

					104. تهديد الأمن العام
					105. تراجع قوة القيم، لردع السلوك المنحرف في المجتمع
					106. لجوء المبتز إلى الضغط على الضحية لارتكاب مخالفات (أخلاقية، قانونية)
					107. تدني الكفاءة الشخصية أكثر لدى الضحية في حلّ مشاكله
					108. خداع الضحية من خلال مشاعر الحب
					109. تراجع ثقة الضحية بنفسه
					110. كره الحياة
					111. تدني مستوى الذكاء العاطفي لدى الضحية " مع العلم بان الذكاء العاطفي يعني قدرة الفرد على مراقبة مشاعره وانفعالاته الذاتية وانفعالات ومشاعر الآخرين والموازنة بينهما".
					112. يتحول مزاج الضحية إلى مزاج حاد يصعب التعامل معه

مع خالص الاحترام والتقدير

اسم الطالبة: نورهان عابدين

إشراف: د. وفاء الخطيب

ملحق (3) أسماء محكمي الاستبانة:

هناك العديد ممن حكموا الاستبانة، الجدول الآتي يتضمن أسمائهم:

الرقم	الاسم	التخصص	مكان العمل
1	د. بدر الأعرج	علم اجتماع	جامعة بيرزيت
2	د. إبراهيم حسنين صبري	تنظيم مجتمع	جامعة حلوان
3	د. محمود الأطرش	علم نفس	جامعة النجاح الوطنية
4	د. محمد برغيت	علم نفس إكلينيكي	جامعة بيرزيت
5	د. خالد هريش	خدمة اجتماعية	جامعة القدس
6	د. صلاح الدين وتد	خدمة اجتماعية	جامعة القدس
7	أ. زياد لافي	محلل إحصائي	جامعة القدس
8	د. علا حسين	تربية وعلم نفس	جامعة القدس
9	د. عبادة ظاهر	علم نفس	الجامعة الأردنية
10	د. عايد وريكات	علم اجتماع	الجامعة الأردنية
11	د. فؤاد طلافحة	محلل إحصائي	جامعة مؤتة
12	د. عصام الأطرش	علم جريمة	كلية الاستقلال
13	د. سمير شقير	تربية وعلم نفس	جامعة القدس

ملحق (4) تسهيل المهمة :

Al-Quds University
Faculty of Arts
Dean's office
Jerusalem – Abu Dies



جامعة القدس
كلية الآداب
مكتب العميد
القدس - أبو ديس

الرقم: ك / أ / ٣٨ / ٢٠١٨

التاريخ: ١٨ / ١٢ / ٢٠١٨

سيادة اللواء حازم عطا الله المحترم
مدير عام الشرطة الفلسطينية

تحية طيبة وبعد،

الموضوع: تسهيل مهمة الطالبة نورهان هاني عابدين رقم جامعي (٢١٥١٠٠٤٦)

ارجو تسهيل عمل الطالبة المذكورة أعلاه بالحصول على المعلومات والإحصائيات وتعبئة الاستبيانات المطلوبة حول الجرائم الإلكترونية في الضفة الغربية، وذلك لغرض إستكمال رسالة الماجستير وعنوانها " الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى مجموعة من الضحايا".

مع فائق الاحترام والتقدير

د. أحمد عياد
عميد الكلية
العميد المساعد/كلية الآداب
منسق برنامج علم الجريمة

Main Campus, Abu-Dies

Tel: 2799753-2796961

Fax: 2791296

الحرم الجامعي الرئيس- أبو ديس

هاتف: 2799753-2796961

فاكس: 2791296

Al-Quds University

Faculty of Arts
MA in Criminology
Jerusalem - Abu Dies



جامعة القدس

كلية الآداب
ماجستير علم الجريمة
القدس - أبو ديس

2018/11/29

عطوفة النائب العام د. أحمد براك المحترم

تحية طيبة وبعد

الموضوع: تسهيل مهمة الطالبة نور هان هاني عابدين رقم جامعي (21510046)

لرجو تسهيل مهمة الطالبة المذكورة أعلاه بالحصول على المعلومات والإحصائيات وتعبئة الاستبانات المطلوبة حول الجرائم الإلكترونية في الضفة الغربية، ولك لغرض إكمال رسالة الماجستير وعنوانها: ' الذكاء العاطفي وعلاقته بممارسة جرائم الإنترنت الإلكتروني لدى مجموعة من الضحايا'.

مع الاحترام

مشرقة الطالبة

د. وفاء الخطيب

Main Campus, Abu- Dies

Tel: 2799753-2796961

Fax: 2791296

الحرم الجامعي الرئيس - أبو ديس

هاتف: 2796961-2799753

فاكس: 2791296

ملحق (5) نتائج المقابلات:

تمّ تحديد مواعيد خاصة مع العاملين في وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية، بما يتناسب مع أوقاتهم من أجل جمع البيانات التي من شأنها أن تساعد في تدعيم نتائج الدراسة الإحصائية.

المقابلة رقم (1)

الجزء الأول: البيانات الشخصية

○ الاسم: سونيا خليل عزاب

○ العمر: 28

○ المستوى التعليمي: بكالوريوس

○ مكان العمل: الشرطة

○ دائرة العمل: وحدة حماية الأسرة، √ وحدة الجرائم الإلكترونية.

○ المسمى الوظيفي: مهندس - مختبر الأدلة الرقمية

○ الرتبة: ملازم أول

○ عدد سنوات الخبرة: 3 سنوات

○ أماكن العمل السابقة: مؤسسة (Jrex)

○ معلومات إضافية ترغب/ين في اطلاعنا عليها:

الجزء الثاني: الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عيّنة من الضحايا .

○ هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟.

3- نعم ✓ 2. لا

○ اذا كانت الإجابة نعم، كيف يكون التأثير؟

اذا كان مستوى الذكاء العاطفي للمجرم عالي يساعده على اختراق عقل الضحية بسهولة واستغلاله عاطفيا بشكل أكبر لوجود القدرة العالية لديه لمعرفة الوضع العاطفي للضحية، وفي حال كان مستوى الذكاء العاطفي للضحية عالي يقلل ذلك من التعرض للابتزاز، واذا كان قليل يكون اسهل للوقوع بالابتزاز.

○ برأيك/ ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفي لدى الضحية؟.

4- نعم ✓ 2. لا

○ اذا كانت الإجابة نعم، كيف يكون التأثير؟

المتغير	يؤثر	لا يؤثر	كيف يؤثر
الجنس	✓		الانثى اسهل للوقوع ضحية
المستوى التعليمي			استهداف الشخص الذي يكون لديه مسمى وظيفي عالي يكون اكثر
مكان السكن	✓		
العمر		✓	اخترق عقل الضحية يكون اسهل
الوظيفة	✓		من ناحية الحاق الضرر يكون عليه اكبر
مستوى الدخل	✓		اذا كان الهدف الحصول على مبلغ مالي
الحالة الاجتماعية	✓		تشكيل افساد رابطة زوجية

الجزء الثالث : جرائم الابتزاز الإلكتروني

○ ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟.
أكثر جرائم الابتزاز الإلكتروني تتمثل في ابتزاز الأنثى من خلال اختراق عقلها بداية واستغلالها عاطفية والحصول على ثقتها وأبرام العهود المستقلة لها وبالتالي الحصول على صور ومقاطع فيديو لها ثم ابتزازها جنسيا أو ماليا وفي حالات كلاهما، بالإضافة إلى ابتزاز الذكور أيضا من خلال الحصول على مقاطع فيديو بإرادته مخلة بالأداب العامة.

○ ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟.

مواقع التواصل الاجتماعيّ كاملة، فيس بوك، تويتر، سناب شات، وغيرها، واتس اب سكايب

○ ما أهم الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟.

1. قلة الوعي لدى الضحية عند التواصل مع شخص عبر الإنترنت وبالتالي الوثوق به وأرسال الصور وفتح الكاميرا، ومقاطع الفيديو.

2. الفراغ وبالتالي استخدام هذه الوسائل بطريقة غير صحيحة

3. الحاجة إلى المال، فيلجا البعض إلى استخدام الابتزاز للحصول على المال

○ هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017)م على التقليل من نسبة جرائم الابتزاز الإلكتروني، كيف ذلك؟.

بشكل عام، نعم، لأنه معرفة الأشخاص بوجود القانون لهذا النوع من الجرائم يكون رادعا لهم لعدم القيام بها، ولكن آلة التعامل مع الجرائم الإلكترونية بشكل عام يتم التحفظ على هذه الجرائم وبالتالي عدم استكمالها قضائيا وهذا يعود لوضع المشتكية تحديدا وعدم رغبتها استكمال الشكوى، لم نلاحظ فرق كبير من ناحية نقصان عدد القضايا من هذا النوع.

○ لماذا تمّ التعديل على قانون رقم (16) لعام (2017)م.؟

*بسبب الادعاء أو الاعتراض على إليه ومجازاة مرتبكي الجريمة أي أن الأحكام المفروضة في القانون عالية ويجب تحقيقها، الجانب أعلامي من ناحية ادعاء الصحفيين بأنه متشدد ويقلص من حرية الراي.

○ ما هو القانون الحالي الذي يتم العمل به مع جرائم الابتزاز الإلكتروني.؟

القانون (10) لعام 2018.

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز الإلكتروني.؟

إجراءات إدارية قانونية حددها قانون الإجراءات الجزائية والقرار بقانون (10) من قانون الجرائم الجزائية

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " لحماية ضحايا جرائم الابتزاز الإلكتروني.؟

تخصص وحدة حماية الأسرة

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا.؟

*الآثار النفسية قد تتأثر الضحية وتحديدا الفتاة نفسيا وذلك بالشعور بفقدان الثقة بالنفس والقدرة على مواجهة المجتمع كالسابق.

*الأثار المادية

○ ما الأثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟.

نظرة المجتمع للوسائل، وسائل التواصل الاجتماعي، وذلك عن قراءة او ملاحظة وجود عدد كبير من هذا النوع من الجرائم ويتم خلال استخدام هذه الوسائل وبالتالي فقدان الثقة.

○ ما هي الصعوبات التي تحد من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

*استخدام الشرائح الإسرائيلية لارتكاب هذه الجرائم وبشكل عام يصعب ملاحقة المرتكبين

*الانقسام الفلسطيني أيضا يشكل صعوبة لملاحقة المرتكبين إذا كان من قطاع غزة

*زيادة استخدام الإنترنت من خلال شرائح 3-G

● من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز الإلكتروني، الرجاء ترتيبها حسب الأولوية؟

8 رقم موحد للتبليغ عن الجرائم الإلكترونية.

4 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

5 الحرص على تقديم الجاني للمحاكمة.

1 حملات توعية مجتمعية.

2 مؤتمرات ومحاضرات.

9 تفعيل دور الرقابة المجتمعية.

3 اكتساب ثقة المواطنين.

6 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.

7 دعم الضحية وحمايته.

غير ذلك حدد/ي:.....

المقابلة رقم (2)

الجزء الأول: البيانات الشخصية

- الاسم: ديماء يوسف عرب
- العمر: 26 سنة
- المستوى التعليمي: حقوق
- مكان العمل: مكتب النائب العام
- دائرة العمل: وحدة حماية الأسرة، √ وحدة الجرائم الإلكترونية.
- المسمى الوظيفي: باحث قانوني
- الرتبة:..
- عدد سنوات الخبرة: سنة
- أماكن العمل السابقة:
- معلومات إضافية ترغب/ين في اطلاعنا عليها:

الجزء الثاني: الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا.

○ هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟.

5- نعم √ لا 2.

○ إذا كانت الإجابة نعم، كيف يكون التأثير؟

العلاقة عكسية بين التعرض للابتزاز الإلكتروني ومستوى الذكاء العاطفيّ، كلما زاد الابتزاز يكون مستوى الذكاء العاطفيّ قليل

○ برأيك/ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفيّ لدى الضحية؟.

6- نعم ✓ لا 2.

○ اذا كانت الإجابة نعم، كيف يكون التأثير؟

المتغير	يؤثر	لا يؤثر	كيف يؤثر
الجنس	✓		على النساء
المستوى التعليمي	✓		يعطي قدر اكبر من الثقة والانفتاح
مكان السكن	✓		تؤثر من حيث التركيبة السكانية
العمر	✓		السن الكبير يعني النضج
الوظيفة	✓		
مستوى الدخل	✓		لاستقلال المالي يرفع من التعرض للابتزاز
الحالة الاجتماعية	✓		يؤثر على النساء بشكل خاص للوضع الاقتصادي السيء

الجزء الثالث : جرائم الابتزاز الإلكتروني

○ ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟.

الإبتراز عن طريق الصور والفيديوهات

○ ما الوسائل المستخدمة للإيقاع بضحايا جريمة الإبتراز الإلكتروني في الضفة الغربية؟.

الإبتراز بكافة أشكاله

○ ما أهم الأسباب التي تؤدي إلى جريمة الإبتراز الإلكتروني حسب القضايا المسجلة لديكم؟.

الضغط الأسري

○ هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017)م على التقليل من نسبة جرائم

الإبتراز الإلكتروني، كيف ذلك؟.

نعم، لوجود مقومات يمكن استخدامها لردع المبتزين وحماية الضحية

○ لماذا تمّ التعديل على قانون رقم (16) لعام (2017)م؟.

لمواكبة التطورات الطارئة التي تحدث للمجتمع

○ ما هو القانون الحالي الذي يتم العمل به مع جرائم الإبتراز الإلكتروني؟.

قانون عام 2018

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة

السلطانية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الإبتراز

الإلكتروني؟.

1. سماع الشكوى

2. التحقيق في الواقعة

3. دراسة الاحتياجات والنتائج

4. وحدة الجرائم الإلكترونية

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة" لحماية ضحايا جرائم الابتزاز الإلكتروني؟.

حماية المعلومات والتعامل بسرية

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟

أضرار اقتصادية، مشاكل في الحياة الزوجية

الخطورة على حياة الضحية

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟.

○ التفكك المجتمعي

○ عدم الإحساس بالمسؤولية

○ عدم الثقة بالتعاملات الاقتصادية مع الآخرين

○ ما هي الصعوبات التي تحد من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في

الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

الخوف من فكرة التحقيق والادعاء امام الوحدة.

• من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز

الإلكتروني، الرجاء ترتيبها حسب الأولوية؟

1 رقم موحد للتبليغ عن الجرائم الإلكترونية.

5 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

6 الحرص على تقديم الجاني للمحاكمة.

2 حملات توعية مجتمعية.

7 مؤتمرات ومحاضرات.

3 تفعيل دور الرقابة المجتمعية.

4 اكتساب ثقة المواطنين.

9 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.

8 دعم الضحية وحمايته.

غير ذلك حدد/ي:.....

المقابلة رقم (3)

الجزء الأول: البيانات الشخصية

- الاسم: جهاد عبد الكريم
- العمر: 48 سنة
- المستوى التعليمي: بكالوريوس
- مكان العمل : الشرطة
- دائرة العمل: \وحدة حماية الأسرة، وحدة الجرائم الإلكترونية.
- المسمى الوظيفي: نائب مدير الإدارة
- الرتبة: عقيد
- عدد سنوات الخبرة: ست سنوات
- أماكن العمل السابقة: التحقيق، الأمن الداخلي، العمليات
- معلومات إضافية ترغب/ين في اطلاعنا عليها .:

الجزء الثاني: الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا .

- هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟.

7- نعم ✓ 2. لا

- اذا كانت الإجابة نعم، كيف يكون التأثير؟

كلما تدنى مستوى الذكاء العاطفي لدى الشخص يؤدي إلى ان يكون عرضه للابتزاز الإلكتروني حيث ان الذكاء العاطفي المتدني يعكس شخصية ضعيفة.

○ برأيك/ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفي لدى الضحية؟.

8- نعم 2. لا ✓

○ اذا كانت الإجابة نعم، كيف يكون التأثير؟

المتغير	يؤثر	لا يؤثر	كيف يؤثر
الجنس			
المستوى التعليمي			
مكان السكن			
العمر			
الوظيفة			
مستوى الدخل			
الحالة الاجتماعية			

الجزء الثالث: جرائم الابتزاز الإلكتروني

- ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟.
- ابتزاز الفتيات من خلال الحصول على صور وفيديوهات لهن أو أي مادة أخرى تلحق بهن الضرر، وغالبا من يكون الهدف مالي
- ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟.

مواقع التواصل الاجتماعي

○ ما أهم الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟.

قلة الوعي وعدم النضج العاطفي.

○ هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017)م على التقليل من نسبة جرائم

الابتزاز الإلكتروني، كيف ذلك؟.

القانون حديثة وتطبيقه يكون رادع للمبتز.

○ لماذا تمّ التعديل على قانون رقم (16) لعام (2017)م؟.

○ ما هو القانون الحالي الذي يتم العمل به مع جرائم الابتزاز الإلكتروني؟.

قانون الجرائم الإلكترونية رقم 16

قانون العقوبات

قانون الإجراءات الجزائية

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة

السلطانية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز

الإلكتروني؟.

لدى إدارة حماية الأسرة يتم استقبال الشكاوي وضبط المواد المستخدمة في الابتزاز وتحويلها لوحدة

الجرائم الإلكترونية لجمع الاستدلالات، ومن ثم تحويل القضية للوحدة العامة المختصة ليتم

الأجراء القانوني بحقه

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " لحماية ضحايا جرائم الابتزاز الإلكتروني؟.

تعمل وحدة حماية الأسرة بعد وحدة الجرائم الإلكترونية لحماية الضحايا إذا كان هناك تقدير يشير بوجود خطر عليهن سواء من المشتبه به أو من الأسر وذلك من خلال إيداع الضحية في مراكز الإيواء وأجراء التدخلات الاجتماعية والنفسية المناسبة.

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟.

وقوع الضحية في دائرة الخطر على حياتها وما يترتب عليها من آثار نفسية واجتماعية

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟.

ازدياد الجريمة وخاصة على الفتيات

خلل في النظام الاجتماعي ناتج عن نقص الثقة

ازدياد هذا النوع من الجرائم يؤدي إلى تكوين ظاهرة وثقافة خطيرة خاصة لدى فئة الشباب والمراهقين يصعب السيطرة عليها في المستقبل.

○ ما هي الصعوبات التي تحد من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

تردد بعض الحالات في اللجوء لإدارة حماية الأسرة لتقديم الشكوى.

نقص الرتب وخاصة من يملكون الخبرة في التعامل في مجال الوسائل الإلكترونية والقانونية.

• من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز الإلكتروني، الرجاء ترتيبها حسب الأولوية؟

2 رقم موحد للتبليغ عن الجرائم الإلكترونية.

3 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

4 الحرص على تقديم الجاني للمحاكمة.

7 حملات توعية مجتمعية.

8 مؤتمرات ومحاضرات.

6 تفعيل دور الرقابة المجتمعية.

1 اكتساب ثقة المواطنين.

9 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.

5 دعم الضحية وحمايته.

○ غير ذلك حدد/ي:

المقابلة رقم (4)

الجزء الأول: البيانات الشخصية

- الاسم: باسل خريوش
- العمر: 49
- المستوى التعليمي: ماجستير
- مكان العمل
- دائرة العمل: \وحدة حماية الأسرة، وحدة الجرائم الإلكترونية.
- المسمى الوظيفي: مدير حماية الأسرة
- الرتبة: مقدم
- عدد سنوات الخبرة: 5.. سنوات
- أماكن العمل السابقة: شرطة نابلس
- معلومات إضافية ترغب/ين في اطلاعنا عليها :.

الجزء الثاني: الذكاء العاطفي وعلاقته بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا

- هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟.

9- نعم لا 2. لا ✓

- إذا كانت الإجابة نعم، كيف يكون التأثير؟

○ برأيك/ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفي لدى الضحية؟.

10- نعم 2. لا

الجزء الثالث : جرائم الابتزاز الإلكتروني

○ ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟.

التشهير

التهديد

لاستغلال

○ ما الوسائل المستخدمة للإيقاع بضحايا جريمة الابتزاز الإلكتروني في الضفة الغربية؟.

الإنترنت

○ ما أهم الأسباب التي تؤدي إلى جريمة الابتزاز الإلكتروني حسب القضايا المسجلة لديكم؟.

العاطفة، الفقر، المشاكل الأسرية

○ هل عمل قانون الجرائم الإلكترونية رقم(16) لعام (2017)م على التقليل من نسبة جرائم

الابتزاز الإلكتروني، كيف ذلك؟.

نعم، كونه رادع

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة

ال فلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز

الإلكتروني؟.

1. استقبال الضحية وسماعها

2. تدوين الإفادة

3. إحالة الملف إلى جهات الاختصاص في وحدة الجرائم الإلكترونية

4. تحويل الملف إلى الوحدة العامة والقضاء

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟.

1. آثار نفسية

2. مشاكل أسرية

3. وجود خطوة على حياة الضحية

4. آثار اقتصادية

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟.

تفكك اسري، عزلة اجتماعية

○ ما هي الصعوبات التي تحد من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في

الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

الموقع الجغرافي بشكل عام يؤدي إلى عدم القدرة على السيطرة

• من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز

الإلكتروني، الرجاء ترتيبها حسب الأولوية؟

4 رقم موحد للتبليغ عن الجرائم الإلكترونية.

1 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

9 الحرص على تقديم الجاني للمحاكمة.

2 حملات توعية مجتمعية.

3 مؤتمرات ومحاضرات.

6 تفعيل دور الرقابة المجتمعية.

5 اكتساب ثقة المواطنين.

8 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.

7 دعم الضحية وحمايته.

غير ذلك حدد/ي:.....

المقابلة رقم (5)

الجزء الأول: البيانات الشخصية

- الاسم: سامر حمد
- العمر: 43
- المستوى التعليمي: بكالوريوس
- مكان العمل: الشرطة
- دائرة العمل: وحدة حماية الأسرة، √ وحدة الجرائم الإلكترونية.
- المسمى الوظيفي:
- الرتبة: عقيد
- عدد سنوات الخبرة: 20.. سنة
- أماكن العمل السابقة: المباحث
- معلومات إضافية ترغب/ين في اطلاعنا عليها :.

الجزء الثاني: ما علاقة الذكاء العاطفي بممارسة جرائم الابتزاز الإلكتروني لدى عينة من الضحايا؟

○ هل يؤثر مستوى الذكاء العاطفي لدى الضحايا على زيادة ممارسة جرائم الابتزاز الإلكتروني؟.

11- نعم √ لا 2.

○ إذا كانت الإجابة نعم، كيف يكون التأثير؟

يؤثر مستوى الذكاء العاطفي من حيث قدرة المبتز على تحليل مشاعر الضحية وفهم قدراته والمشاكل التي يعاني منها وهذا يكون مدخل لمعرفة كيفية الاحتيال عليها ثم الحصول على البيانات اللازمة

○ برأيك/ك هل تؤثر البيانات الشخصية والديموغرافية اللاحقة على مستوى الذكاء العاطفي لدى الضحية؟.

12- نعم ✓ لا 2.

○ اذا كانت الإجابة نعم، كيف يكون التأثير؟

المتغير	يؤثر	لا يؤثر	كيف يؤثر
الجنس	✓		على النساء
المستوى التعليمي	✓		كلما كان المستوى التعليمي اعلى يؤثر اكثر
مكان السكن		✓	
العمر	✓		الفئات العمرية الكبيرة
الوظيفة	✓		الوظيفة اعلى
مستوى الدخل	✓		الدخل المادي المرتفع
الحالة الاجتماعية	✓		الوضع الاسري

الجزء الثالث : جرائم الابتزاز الإلكتروني

○ ما هي أكثر أنواع جرائم الابتزاز الإلكتروني التي تتعاملون معها في مجال عملكم؟.

الإبتيزاز المالي، والجنسي

○ ما الوسائل المستخدمة للإيقاع بضحايا جريمة الإبتيزاز الإلكتروني في الضفة الغربية؟.

الإيقاع بالضحية من خلال حساب وهمي وممارسة الجنس من خلال الكاميرا عبر برامج الدردشة ولاحقا إبتيزاز الضحية بالتسجيلات وأنه سيتم نشرها على الأقارب والأصحاب في حالة عدم الرضوخ للإبتيزاز

○ ما أهم الأسباب التي تؤدي إلى جريمة الإبتيزاز الإلكتروني حسب القضايا المسجلة لديكم؟.

1. الجهل وقلة الوعي

2. عدم الحفاظ على الخصوصية

3. الجريمة الإلكترونية

4. عدم وجود هيئات قضائية مختصة

5. الانقسام واستغلاله

6. الوضع المادي السيء

○ هل عمل قانون الجرائم الإلكترونية رقم (16) لعام (2017)م على التقليل من نسبة جرائم الإبتيزاز الإلكتروني، كيف ذلك؟.

القانون لم يختبر حتى الآن

○ لماذا تمّ التعديل على قانون رقم (16) لعام (2017)م؟.

من باب التحديث وحسب الحاجة

○ ما هو القانون الحالي الذي يتم العمل به مع جرائم الإبتيزاز الإلكتروني ؟.

10 لسنة 2018

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " في التعامل مع جرائم الابتزاز الإلكتروني؟.

إدارية ترتبط بالقانون والإجراءات الجزائية

وفنية وترتبط بعمل الأدوات المستخدمة ويتم الفحص من خلال الأدوات.

○ ما هي الإجراءات المتبعة من "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة " لحماية ضحايا جرائم الابتزاز الإلكتروني؟.

الحماية هي من صلاحيات وحدة حماية الأسرة

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني لدى الضحايا؟.

تؤثر على الأسرة وتساهم في التفكك الأسري

قد تؤدي بحياة الضحية في بعض الحالات

○ ما الآثار الناجمة عن جرائم الابتزاز الإلكتروني على المجتمع؟.

تؤثر على الأسرة وتساهم في التفكك الأسري وقد تؤدي بحياة الضحية

فقدان الثقة

مشاكل اجتماعية وتفكك اسري

○ ما هي الصعوبات التي تحد من عمل "وحدة الجرائم الإلكترونية ووحدة حماية الأسرة في الشرطة الفلسطينية ونيابة الجرائم الإلكترونية في النيابة العامة"، من وجهة نظرك/ي؟

كونها جريمة جديدة تحتاج إلى دقة وخبرة في التعامل معها. كما ان استخدام الشرائح الاسرائيلية.

• من وجهة نظرك ما هي الآليات التي يمكن أن تساعد في الحد من ممارسة جريمة الابتزاز الإلكتروني، الرجاء ترتيبها حسب الأولوية؟

7 رقم موحد للتبليغ عن الجرائم الإلكترونية.

3 تطبيق قانون الجرائم الإلكترونية المعدل على كافة الأفراد بما يتضمنه من عقوبات.

3 الحرص على تقديم الجاني للمحاكمة.

2 حملات توعية مجتمعية.

2 مؤتمرات ومحاضرات.

6 تفعيل دور الرقابة المجتمعية.

1 اكتساب ثقة المواطنين.

5 نشر قصص نجاح للتأكيد على أهمية التدخل المهني.

4 دعم الضحية وحمايته.

غير ذلك حدد/ي:

ملحق (6) قانون رقم (10) لسنة (2017):

قرار بقانون رقم (16) لسنة 2017م بشأن الجرائم الإلكترونية

رئيس دولة فلسطين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

استنادا لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على قانون رقم (74) لسنة 1963م وتعديلاته، الساري في المحافظات الجنوبية، وعلى أحكام قانون العقوبات الأردني رقم (16) لسنة 1960م وتعديلاته، الساري في المحافظات الشمالية،

وعلى قانون رقم (3) لسنة 1996م، بشأن الاتصالات السلكية واللاسلكية،

وعلى قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته،

وعلى القرار بقانون رقم (18) لسنة 2015م، بشأن مكافحة المخدرات والمؤثرات العقلية،

وعلى قرار بقانون رقم (20) لسنة 2015م، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته،

وبناءً على تنسيب مجلس الوزراء بتاريخ 2017/06/20م،

وعلى الصلاحيات المخولة لنا،

وتحقيقاً للمصلحة العامة،

وباسم الشعب العربي الفلسطيني،

أصدرنا القرار بقانون الآتي

مادة (1)

يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك :

الوزارة :وزارة الاتصالات وتكنولوجيا المعلومات .

الوزير :وزير الاتصالات وتكنولوجيا المعلومات .

معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات سواء تعلقت بأفراد أو خلافة، بما في ذلك جمع تلك البيانات، أو استلامها، أو تسجيلها، أو تخزينها، أو تعديلها، أو نقلها، أو استرجاعها، أو محوها، أو نشرها، أو إعادة نشر بيانات، أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤه أو تعديل محتوياته .

تكنولوجيا المعلومات: هي أية وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أية وسيلة أخرى سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، ويشمل أية قدرة تخزين بيانات، أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة .

البيانات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها .

المعلومات الإلكترونية: أية معلومة يمكن تخزينها ومعالجتها وتوريدها ونقلها بوسائل تكنولوجيا المعلومات بوجه خاص بالكتابة، أو الصور، أو الصوت، أو الأرقام، أو الحروف، أو الرموز، أو الإشارات، وغيرها .

الشبكة الإلكترونية: هي ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت).

السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفا لحالة تتعلق بشخص أو شيء ما؛ والتي يتم إنشاؤها، أو إرسالها، أو تسلمها، أو تخزينها بوسائل إلكترونية .

المستند الإلكتروني: هو السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينها أو استخراجها أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه .

الموقع الإلكتروني: هو مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد .

الشخص: الشخص الطبيعي أو المعنوي .

التطبيق الإلكتروني: هو برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر؛ يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها .

بيانات المرور: أية بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته ونوع خدمة الاتصال .

كلمة السر: هي كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات وما في حكمها للتأكد من هويته وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها .

وسيلة التعامل الإلكتروني: هي البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك .

البيانات الحكومية: يشمل ذلك بيانات الدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها .

التشفير: هو تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية .

الشفرة: هي مفتاح، أو مفاتيح سرية خاصة، لشخص أو لجهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز أو ما في حكمها .

الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها .

الاختراق: هو الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية .

التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها ويميزه عن غيره بغرض الموافقة على مضمون المعاملة .

أداة التوقيع: هي برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة .

الشهادة: شهادة التصديق الإلكترونية التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني .

مزود الخدمة: هو أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب وحدة عن أية خدمة إلكترونية أو مستخدمى هذه الخدمة .

الإتلاف: هو تدمير البرامج الإلكترونية سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالحة للاستعمال .

معلومات المشترك: أية معلومة موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات بما في ذلك :

- نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.
- هوية المشترك وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة.
- أية معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة.

الموظف: كل من يعمل في القطاع العام، أو الخاص، أو المؤسسات الخاصة، أو الهيئات المحلية والأهلية، أو الجمعيات، أو الشركات الخاصة التي تساهم بها الدولة، وكل من هو في حكمهم .

مادة (2)

1. تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء أكان الفاعل أصلياً، أم شريكاً، أم محرضاً، أم متدخلًا، على أن تكون الجرائم معاقبا عليها خارج فلسطين مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ.

2. يجوز ملاحقة كل من يرتكب خارج فلسطين إحدى الجرائم المنصوص عليها بهذا القرار بقانون في إحدى الحالات الآتية:

أ. إذا ارتكبت من مواطن فلسطيني .

ب. إذا ارتكبت ضدّ أطراف أو مصالح فلسطينية .

ج. إذا ارتكبت ضدّ أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد في الأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية .

مادة (3)

1. تنشأ وحدة متخصصة في الجرائم الإلكترونية في الأجهزة الشرطة وقوى الأمن على أن تتمتع بصفة الضابطة القضائية، وتتولى الوحدة العامة الإشراف على مأموري الضبط القضائي كل في دائرة اختصاصه.
2. تتولى المحاكم النظامية والوحدة العامة، وفقاً لاختصاصاتهما، بالنظر في دعاوى الجرائم الإلكترونية.

مادة (4)

1. كل من دخل عمدا وبدون وجه حق بأية وسيلة موقعا 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 نشرها، أو إلحاق ضرر 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 القوائم على إدارته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

4. إذا ارتكب الفعل المحدد في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (5)

كل من أعاق أو عطل الوصول إلى الخدمة، أو الدخول إلى الأجهزة، أو البرامج أو مصادر البيانات، أو المعلومات، بأية وسيلة كانت عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً، أو بالعقوبتين كليهما .

مادة (6)

كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل، أو تعطيلها، أو تدمير البرامج، أو حذفها، أو 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 بالعملة المتداولة قانوناً .

مادة (7)

كل من النقط ما هو مرسل عن طريق الشبكة، أو إحدى وسائل تكنولوجيا المعلومات، أو سجله، أو اعترضه، أو تتصت 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 .

مادة (8)

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.

1. 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.
2. كل من ارتكب جريمة باستخدام أي من المذكور في الفقرة (2) من هذه المادة، يعاقب بالأشغال الشاقة المؤقتة وبالغرامة التي لا تقل عن ألفي دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (9)

1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بالغرامة التي لا تقل عن خمسمائة دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين 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 تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كليهما.

المادة (10)

كل من قام عمداً بإنشاء أو نشر شهادة غير صحيحة، أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة، أو إلغائها أو إيقافها، يعاقب بالحبس وبالغرامة التي لا تقل عن مائتي دينار أردني ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (11)

1. كل من زور مستندا 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 كليهما.
3. كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة التزوير حسب الأصول.
4. كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه، أو إتلافه، أو تعييبه، أو تعديله، أو تحويره، أو بأية طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته، أو معلوماته، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات وبالغرامة التي لا تقل عن خمسة آلاف دينار أردني، ولا تزيد عن عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً.
5. إذا وقع التزوير أو التلاعب فيما عدا ذلك من التواقيع الإلكترونية في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد عن ثلاثة آلاف دينار أردني، أو بالعقوبتين كليهما.
6. كل من أنشا 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 كليهما.

مادة (12)

1. كل من استخدم الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات في الوصول دون وجه حق إلى أرقام، أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن خمسمائة دينار أردني ولا تزيد على ثلاثة آلاف دينار أردني، أو بالعقوبتين كليهما.
2. كل من زور وسيلة تعامل إلكترونية بأية وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
3. كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك، أو قبل وسيلة تعامل إلكترونية غير سارية، أو مزورة، أو مسروقة، أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة.
4. إذا قصد من ذلك استخدامها في الحصول على أموال أو بيانات غيره أو ما تنتجها من خدمات، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما.

5. إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال غيره، يعاقب مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما.

مادة (13)

كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال، أو اختلاسها يعاقب بالأشغال الشاقة المؤقتة، أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني أو بالعقوبتين كليهما .

مادة (14)

كل من توصل عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات إلى الاستيلاء لنفسه، أو لغيره على مال منقول، أو على سند، أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني، أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كليهما .

مادة (15)

1. كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كليهما.

2. إذا كان التهديد بارتكاب جريمة أو بإسناد أمور خادشة للشرف والاعتبار، يعاقب بالأشغال الشاقة المؤقتة وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (16)

1. كل من أنتج ما من شأنه المساس بالآداب العامة، أو أعده أو هيأه أو أرسله أو خزنه بقصد الاستغلال، أو التوزيع أو العرض على غيره عن طريق الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، أو الرسوم

المتحركة، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كليهما.

2. كل من أنشا موقعا أو تطبيقا أو حسابا 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 مالية لا تقل عن ألف دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو بالعقوبتين كليهما.

3. إذا كان الفعل المحدد في الفقرتين (1،2) 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.

مادة (17)

كل من أنشا موقعا أو تطبيقا أو حسابا إلكترونياً أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الاتجار في البشر والأعضاء البشرية أو تسهيل التعامل فيه، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (18)

دون الإخلال بالأحكام الواردة في قرار بقانون مكافحة غسل الأموال وتمويل الإرهاب، كل من أنشا 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 عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (19)

كل من أنشا موقعا على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات والمؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو لبيعها، أو شرح، أو عرض طرق إنتاج المواد المخدرة، يعاقب بالحبس مدة لا تقل عن عشر سنوات، وبغرامة لا تقل عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (20)

1. كل من أنشا موقعا 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 كلتيهما.
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 كلتيهما.
3. إذا كان الفعل الوارد في الفقرتين (1،2) من هذه المادة في حالة الطوارئ تضاعف العقوبة المقررة له.

مادة (21)

كل من أنشا موقعا، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات بقصد الإساءة أو سب إحدى المقدسات أو الشعائر المقررة للأديان، أو أحد المعتقدات الدينية، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن ألفي دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كلتيهما .

مادة (22)

كل من أنشا موقعا، 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 أكانت مباشرة أو مسجلة تتصل بحرمة الحياة الخاصة، أو العائلية للأفراد ولو كانت صحيحة، أو تعدى بالدم، أو القرح، أو التحقير أو التشهير بالآخرين وإلحاق الضرر بهم، يعاقب بالحبس

مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كليهما .

مادة (23)

كل من أنشا موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة، أو تسهيله، أو تشجيعه، أو الترويج له، أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة شهور، أو بغرامة لا تقل عن ألف دينار أردني ولا تزيد على خمسة آلاف دينار أردني، أو بالعقوبتين كليهما .

مادة (24)

كل من أنشا موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد نشر وتوزيع معلومات تنثير النعرات العنصرية، وتهدف إلى التمييز العنصري بحق فئة معينة، أو أقدم على تهديد شخص، أو تحقيره، أو التعدي عليه بسبب انتمائه العرقي أو المذهبي، أو اللون، أو الشكل، أو سبب الإعاقة، يعاقب بالأشغال الشاقة المؤقتة، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشر آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (25)

كل من أنشا موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التبرير لأعمال إبادة جماعية، أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية، أو المساعدة قسداً، أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالأشغال الشاقة المؤبدة، أو الأشغال الشاقة المؤقتة مدة لا تقل عن عشر سنوات .

مادة (26)

كل من حاز جهازاً بغرض الاستخدام، أو برنامجاً، أو أية بيانات إلكترونية معدة، أو كلمة سر، أو ترميز دخول، أو قدمها، أو أنتجها، أو وزعها، أو استورها، أو صدرها، أو روج لها، وذلك بغرض اعتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالأشغال الشاقة المؤقتة مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (27)

1. كل موظف ارتكب أياً من الجرائم المنصوص عليها في هذا القرار بقانون مستغلاً صلاحياته وسلطته في أثناء تأدية عمله، أو بسببها أو سهل ذلك لغيره، يعاقب بالحبس مدة لا تقل عن سنة أو بغرامة لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، أو بالعقوبتين كليهما.
2. كل من ارتكب من موظفي مزودي الخدمة، أياً من الجرائم المنصوص عليها في هذا القرار بقانون في أثناء تأدية عمله، أو بسببها، أو سهل ذلك لغيره، يعاقب بالأشغال الشاقة المؤقتة مدة لا تقل عن ثلاث سنوات، أو بغرامة لا تقل عن عشرة آلاف دينار أردني ولا تزيد على عشرين ألف دينار أردني، أو بالعقوبتين كليهما.

مادة (28)

كل من أنشأ موقعاً، أو تطبيقاً، أو حساباً إلكترونياً، أو نشر معلومات على الشبكة الإلكترونية، أو إهدى وسائل تكنولوجيا المعلومات؛ بقصد ارتكاب أية جريمة يعاقب عليها بموجب أي تشريع نافذ، أو اشترك أو حرض على ارتكابها، يعاقب بضعف العقوبة المنصوص عليها في ذلك التشريع .

مادة (29)

1. كل من حرض، أو ساعد، أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون بأية وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة، أو الاتفاق، يعاقب بنثلي الحد الأقصى للعقوبة المقررة لفاعلها.
2. إذا كان المجني عليه طفلاً في الفقرة (1) من هذه المادة، يعاقب المجرم بالأشغال الشاقة المؤقتة مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ألفي دينار أردني ولا تزيد عن خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، ولو لم تقع الجريمة فعلاً.

مادة (30)

إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالغرامة التي لا تقل عن خمسة آلاف دينار أردني ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات، أو أن تقضي بحله وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له .

مادة (31)

يعاقب بالحبس مدة لا تقل عن ثلاثة شهور، وبغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني كلّ من قام باستخدام أنظمة أو موقع أو تطبيق إلكتروني؛ لتجاوز الحجب المفروض بموجب أحكام هذا القرار بقانون .

مادة (32)

يلتزم مزود الخدمة، وفقا للإجراءات القانونية المقررة بالآتي :

1. تزويد الجهات المختصة بجميع البيانات والمعلومات اللازمة التي تساعد في كشف الحقيقة، بناءً على طلب الوحدة أو المحكمة المختصة.
2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية مع مراعاة الإجراءات الواردة في المادة (40) من هذا القرار بقانون.
3. الاحتفاظ بالمعلومات عن المشترك لمدة لا تقل عن ثلاث سنوات.
4. التعاون ومساعدة الجهات المختصة، وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ بها.

مادة (33)

1. للوحدة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة.
2. يجب أن يكون أمر التفتيش مسببا ومحدداً، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة.
3. إذا أسفر التفتيش المحدد في الفقرة (2) من هذه المادة عن ضبط أجهزة، أو أدوات، أو وسائل ذات صلة بالجريمة؛ يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات وعرضها على الوحدة العامة لاتخاذ ما يلزم بشأنها.
4. لوكليل الوحدة العامة أن يأذن بالنفاز المباشر لمأموري الضبط القضائي، أو من يستعينون بهم من أهل الخبرة إلى أية وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات.

5. يشترط في مأمور الضبط القضائي أن يكون مؤهلاً للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية.

مادة (34)

1. للوحدة العامة الحصول على الأجهزة، أو الأدوات، أو الوسائل، أو البيانات، أو المعلومات الإلكترونية، أو بيانات المرور، أو البيانات المتعلقة بحركة الاتصالات، أو بمستعملها أو معلومات المحتوى ذات الصلة بالجريمة الإلكترونية.
2. للوحدة العامة الإذن بالضبط والتحفيز على كامل نظام المعلومات، أو جزء منه، أو أية وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة.
3. إذا لم يكن الضبط والتحفيز على نظام المعلومات ضرورياً، أو تعذر إجراؤه؛ تنسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات.
4. إذا استحال إجراء الضبط والتحفيز عليه بصفة فعلية؛ وحفاظاً على أدلة الجريمة يتعين استعمال كافة الوسائل المناسبة؛ لمنع الوصول والنفاد إلى البيانات المخزنة بنظام المعلومات.
5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفز عليه بما في ذلك الوسائل الفنية لحماية محتواها.
6. تحرر قدر الإمكان قائمة بالمضبوط المتحفز عليه بحضور المتهم، أو من وجد لديه المضبوط المتحفز عليه، ويحرر تقرير بذلك، ويُحفظ المضبوط المتحفز عليه حسب الحالة في ظرف، أو مغلف مختوم، وتكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية.

مادة (35)

1. لقاضي الصلح أن يأذن للوحدة العامة بمراقبة الاتصالات والمحادثات الإلكترونية وتسجيلها والتعامل معها؛ للبحث عن الدليل المتعلق بالجريمة وذلك لمدة خمسة عشر يوماً قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جديدة، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضراً بذلك يقدمه إلى الوحدة العامة.
2. للوحدة العامة أن تأمر بالجمع والتزويد الفوري لأي بيانات بما فيها حركات الاتصالات، أو معلومات إلكترونية، أو بيانات مرور، أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات، باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمة حسب نوع الخدمة التي يقدمها.

مادة (36)

على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة، أو الأدوات، أو وسائل تكنولوجيا المعلومات، أو الأنظمة الإلكترونية، أو البيانات، أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها .

مادة (37)

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له ومدته.
2. تكون مدة الاعتراض المحدد في الفقرة (1) من هذه المادة ثلاثة شهور من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط.
3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام الوحدة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها.

مادة (38)

لا يجوز استبعاد أي دليل ناتج عن وسيلة من وسائل تكنولوجيا المعلومات، أو أنظمة المعلومات، أو شبكات المعلومات، أو المواقع الإلكترونية، أو البيانات والمعلومات الإلكترونية، بسبب طبيعة ذلك الدليل .

مادة (39)

لا يجوز استبعاد أي من الأدلة المتحصل عليها بمعرفة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى لمجرد ذلك السبب، طالما أن الحصول عليها قد تمّ وفقاً للإجراءات القانونية والقضائية للتعاون الدولي .

مادة (40)

1. لجهات التحري والضبط المختصة - إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أية عبارات، أو أرقام، أو صور، أو أفلام، أو أية مواد دعائية، أو غيرها، من شأنها تهديد الأمن

القومي، أو السلم الأهلي، أو النظام العام، أو الآداب العامة - أن تعرض محضرا بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية، أو حجب بعض روابطها من العرض.

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

مادة (41)

فيما عدا الالتزامات المهنية المنصوص عليها في القانون لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها؛ للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقا لأحكام القانون .

مادة (42)

تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بما يلي :

1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية وشبكاتها المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها.
2. الإسراع في إبلاغ الجهة المختصة عن أية جريمة منصوص عليها في هذا القرار بقانون فور اكتشافها أو اكتشاف أية محاولة للانتقاط، أو الاعتراض، أو التنصت بشكل غير مشروع وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة.
3. الاحتفاظ ببيانات تكنولوجيا المعلومات ومعلومات المشترك لمدة لا تقل عن 120 يوما وتزويد الجهة المختصة بتلك البيانات.
4. التعاون مع الجهات المختصة لتنفيذ اختصاصاتها.

مادة (43)

1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال وتفاذي ارتكابها والمساعدة على التحقيق فيها وتتبع مرتكبيها.

2. يتوقف التعاون المشار إليه بالفقرة (1) من هذه المادة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون.

مادة (44)

1. يتعين على الجهات المختصة أن تقدم العون للجهات النظرية في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقا للقواعد التي يقرها قانون الإجراءات الجزائية والإتفاقيات الثنائية، أو متعددة الأطراف التي تكون الدولة طرفا فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر.

2. لا ينفذ طلب المساعدة القانونية، أو طلب تسليم المجرمين، استنادا إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة طالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة طالبة تدرج الجريمة في فئة الجرائم ذاتها، أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرما بمقتضى قوانين الدولة طالبة.

مادة (45)

مع عدم الإخلال بأية عقوبة أشد ينص عليها قانون العقوبات النافذ، أو أي قانون آخر يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات المنصوص عليها فيه .

مادة (46)

كل من ارتكب فعلا يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها، أو تدخل، أو حرض على ارتكابها، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع .

مادة (47)

كل من أنشا موقعا على الشبكة الإلكترونية، يهدف إلى الترويج لارتكاب أية جريمة من الجرائم المنصوص عليها في قانون العقوبات، أو أي من القوانين الخاصة، يعاقب بالسجن المؤقت وبغرامة لا تقل عن خمسة آلاف دينار ولا تزيد على عشرة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (48)

كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس وبغرامة لا تقل عن خمسمائة دينار ولا تزيد على ثلاثة آلاف دينار أردني أو بإحدى هاتين العقوبتين .

مادة (49)

كل من أقدم على العبث بأدلة قضائية معلوماتية، أو أقدم على إتلافها، أو إخفائها، أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (50)

كل من امتنع عن قصد في الإبلاغ، أو أبلغ عن قصد بشكل خاطئ عن جرائم معلوماتية، يعاقب بالحبس مدة لا تقل عن ستة شهور، وبغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني أو بإحدى هاتين العقوبتين .

مادة (51)

إذا وقعت أية جريمة من الجرائم المنصوص عليها في هذا القرار بقانون بغرض الإخلال بالنظام العام، أو تعريض سلامة المجتمع وأمنه للخطر، أو تعريض حياة المواطنين للخطر، أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القانون الأساسي أو القوانين أو اللوائح، أو بقصد الإضرار بالوحدة الوطنية، والسلام الاجتماعي، أو ازدياد الأديان أو الاعتداء على الحقوق والحريات التي يكفلها الدستور أو القانون الأساسي، تكون العقوبة الأشغال الشاقة المؤبدة أو المؤقتة .

مادة (52)

يعاقب من يشترك بطريق الاتفاق أو التحريض، أو المساعدة، أو التدخل في ارتكاب جنائية، أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب عليها بنصف العقوبة المقررة لها .

مادة (53)

يعد مرتكبا لجريمة الشروع كلّ من شرع في ارتكاب جنائية أو جنحة من الجرائم المنصوص عليها، في هذا القرار بقانون ويعاقب بنصف العقوبة المقررة لها .

مادة (54)

1. دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حسن النية، تصدر المحكمة قرارا بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون، أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل.
2. تصدر المحكمة قرارا بمدّة إغلاق المحل وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال.

مادة (55)

تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أيا من الجرائم المنصوص عليها فيه سواء ارتكبت في فلسطين أم خارجها، وتعتبر الأحكام الأجنبية سابقة التكرار بحق الجاني .

مادة (56)

تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون في أي من الحالات الآتية :

1. إذا ارتكبها أو سهل ارتكابها موظف في مؤسسة خاصة، أو موظف عام مستغلا صلاحياته وسلطاته في ذلك، أو من في حكمه، كما يحكم على الموظف العام بالفصل من الوظيفة في حال الإدانة.

2. إذا وقعت الجريمة على موقع، أو نظام معلوماتي، أو بيانات، أو أرقام، أو حروف، أو شفرات، أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها بما في ذلك الهيئات المحلية.
3. ارتكاب الجاني الجريمة من خلال عصابة منظمة.
4. التهجير بالأحداث ومن في حكمهم واستغلالهم.
5. إذا وقعت الجريمة على نظام معلومات، أو موقع إلكتروني، أو شبكة معلوماتية تتعلق بتحويل الأموال، أو بتقديم خدمات الدفع والتقاص، أو التسويات أو بأي من الخدمات المصرفية المقدمة من البنوك والشركات المالية.

مادة (57)

يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كل من بادر من الجناة بإبلاغ السلطات المختصة بأية معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة وأدى إلى ضبط باقي الجناة .

مادة (58)

تتولى الوزارة وفقا لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون .

مادة (59)

يلغى كل ما يتعارض مع أحكام هذا القرار بقانون .

مادة (60)

يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره .

مادة (61)

على الجهات المختصة كافة، كلّ فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية .

صدر في مدينة رام الله بتاريخ: 2017/06/24 ميلادية

الموافق: 29/رمضان/2017 هجرية

محمود عباس

رئيس دولة فلسطين

رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية

ملحق (7) قانون رقم (10) لسنة 2018:

رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية استنادا لأحكام القانون الأساسي المعدل لسنة 2003م وتعديلاته، لا سيما أحكام المادة (43) منه، وبعد الاطلاع على أحكام قانون العقوبات رقم (74) لسنة 1936م وتعديلاته، الساري في المحافظات الجنوبية، والاطلاع على أحكام قانون العقوبات رقم (16) لسنة 1960م وتعديلاته الساري في المحافظات الشمالية، وعلى أحكام قانون الاتصالات السلكية واللاسلكية رقم (3) لسنة 1996م وعلى أحكام قانون الإجراءات الجزائية رقم (3) لسنة 2001م وتعديلاته وعلى أحكام القرار بقانون رقم (18) لسنة 2015م، بشأن مكافحة المخدرات والمؤثرات العقلية، وعلى أحكام القرار بقانون رقم (20) لسنة 2015م، بشأن مكافحة غسل الأموال وتمويل الإرهاب وتعديلاته، وعلى أحكام القرار بقانون رقم (6) لسنة 2017م، بشأن تنظيم نقل وزراعة الأعضاء البشرية، وعلى أحكام القرار بقانون رقم (15) لسنة 2017م، بشأن المعاملات الإلكترونية، وعلى أحكام القرار بقانون رقم (16) لسنة 2017م، بشأن الجرائم الإلكترونية، وبناءً على تسيب مجلس الوزراء بتاريخ 2018/04/17م، وعلى الصلاحيات المخولة لنا، وتحقيقاً للمصلحة العامة، وباسم الشعب العربي الفلسطيني، أصدرنا القرار بقانون الآتي :

مادة (1)

يكون للكلمات والعبارات الواردة في هذا القرار بقانون المعاني المخصصة لها أدناه، ما لم تدل القرينة على خلاف ذلك :الوزارة: وزارة الاتصالات وتكنولوجيا المعلومات .الوزير: وزير الاتصالات وتكنولوجيا المعلومات .معالجة البيانات: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات، سواء تعلقت بأفراد أو خلافه، بما في ذلك جمع تلك البيانات أو استلامها أو تسجيلها أو تخزينها أو تعديلها أو نقلها أو استرجاعها أو محوها أو نشرها، أو إعادة نشر بيانات أو حجب الوصول إليها، أو إيقاف عمل الأجهزة أو إلغاؤها أو تعديل محتوياتها .تكنولوجيا المعلومات: أي وسيلة إلكترونية مغناطيسية بصرية كهروكيميائية، أو أي وسيلة أخرى، سواء أكانت مادية أم غير مادية، أو مجموعة وسائل مترابطة أو غير مترابطة، تستخدم لمعالجة البيانات وأداء المنطق والحساب أو الوظائف التخزينية، وتشمل أي قدرة تخزين بيانات أو اتصالات تتعلق أو تعمل بالاقتران مع مثل هذه الوسيلة .البيانات والمعلومات الإلكترونية: كل ما يمكن تخزينه أو معالجته أو إنشاؤه أو توريده أو نقله باستخدام تكنولوجيا المعلومات، بوجه خاص الكتابة أو الصور أو الصوت أو الأرقام أو الحروف أو الرموز أو الإشارات، وغيرها . الشبكة الإلكترونية: ارتباط بين أكثر من وسيلة لتكنولوجيا المعلومات للحصول على المعلومات وتبادلها، بما في ذلك الشبكات الخاصة أو العامة أو الشبكة العالمية (الإنترنت) .(السجل الإلكتروني: مجموعة المعلومات التي تشكل بمجملها وصفا لحالة تتعلق بشخص أو شيء ما، والتي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها

بوسائل إلكترونية. المستند الإلكتروني: السجل الإلكتروني الذي يصدر باستخدام إحدى وسائل تكنولوجيا المعلومات، يتم إنشاؤه أو تخزينه أو استخراجة أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة تكنولوجيا المعلومات على وسيط مادي أو على أي وسيط إلكتروني آخر، ويكون قابلاً للاسترجاع بشكل يمكن فهمه. الموقع الإلكتروني: مكان إتاحة المعلومات أو الخدمات على الشبكة الإلكترونية من خلال عنوان محدد. الشخص: الشخص الطبيعي أو المعنوي. التطبيق الإلكتروني: برنامج إلكتروني مصمم لأداء مهمة محددة بشكل مباشر للمستخدم أو لبرنامج إلكتروني آخر، يستخدم من خلال وسائل تكنولوجيا المعلومات أو ما في حكمها. بيانات المرور: أي بيانات أو معلومات إلكترونية تنشأ عن طريق تكنولوجيا المعلومات تبين مصدر الإرسال، والوجهة المرسل إليها، والطريق الذي سلكه، ووقته، وتاريخه، وحجمه، ومدته، ونوع خدمة الاتصال. كلمة السر: كل ما يستخدم للولوج لنظم تكنولوجيا المعلومات، وما في حكمها، للتأكد من هويته، وهي جزء من بيانات المرور، وتشمل الرموز وبصمة العين أو الوجه أو الأصبع أو ما في حكمها. وسيلة التعامل الإلكتروني: البطاقة الإلكترونية التي تحتوي على شريط ممغنط أو شريحة ذكية أو ما في حكمها من تكنولوجيا المعلومات أو تطبيق إلكتروني، تحتوي هذه الوسيلة على بيانات أو معلومات إلكترونية تصدرها الجهات المرخصة بذلك. البيانات الحكومية: البيانات الخاصة بالدولة والهيئات والمؤسسات العامة أو الشركات التابعة لها. التشفير: تحويل بيانات إلكترونية إلى شكل يستحيل به قراءتها وفهمها دون إعادتها إلى هيئتها الأصلية. الشفرة: مفتاح أو مفاتيح سرية خاصة، لشخص أو جهة معينة تستخدم لتشفير البيانات الحاسوبية بالأرقام والحروف والرموز والبصمات أو ما في حكمها. الالتقاط: مشاهدة البيانات أو المعلومات أو الحصول عليها. الاختراق: الدخول غير المصرح به أو غير المشروع لنظم تكنولوجيا المعلومات أو الشبكة الإلكترونية. التوقيع الإلكتروني: بيانات إلكترونية مضافة أو ملحقة أو مرتبطة بمعاملة إلكترونية، ولها طابع يسمح بتحديد هوية الشخص الذي وقعها، ويميزه عن غيره بغرض الموافقة على مضمون المعاملة. أداة التوقيع: برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة. الشهادة: شهادة التصديق الإلكتروني التي تصدرها الوزارة أو الجهة المفوضة من قبلها لإثبات العلاقة والارتباط بين الموقع وبيانات التوقيع الإلكتروني. مزود الخدمة: أي شخص يقدم لمستخدمي الخدمة الخاصة به القدرة على الاتصال عن طريق تكنولوجيا المعلومات، أو أي شخص آخر يقوم بمعالجة أو تخزين أو استضافة بيانات الحاسوب وحدة عن أي خدمة إلكترونية أو مستخدم هذه الخدمة. الإلتلاف: تدمير البرامج الإلكترونية، سواء أكان كلياً أم جزئياً، أو جعلها على نحو غير صالح للاستعمال. معلومات المشترك: المعلومات الموجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات حول نوع خدمة الاتصالات المستخدمة، والشروط الفنية، وفترة الخدمة، وهوية المشترك، وعنوانه البريدي أو الجغرافي أو هاتفه، ومعلومات الدفع المتوفرة بناءً على اتفاق أو تركيب الخدمة، وأي معلومات أخرى عن موقع تركيب معدات الاتصال بناءً على اتفاق الخدمة. الموظف: كل من يعمل في القطاع العام أو الخاص أو المؤسسات الخاصة أو الهيئات المحلية والأهلية أو الجمعيات أو الشركات الخاصة التي تساهم بها

الدولة، وكل من هو في حكمهم .الحبس: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين أسبوع إلى ثلاث سنوات .السجن: وضع المحكوم عليه بحكم قضائي في أحد سجون الدولة مدة تتراوح بين ثلاث سنوات إلى خمس عشرة سنة .

مادة (2)

1.تطبق أحكام هذا القرار بقانون على أي من الجرائم المنصوص عليها فيه، إذا ارتكبت كلياً أو جزئياً داخل فلسطين أو خارجها، أو امتد أثرها داخل فلسطين، سواء كان الفاعل أصلياً أم شريكاً أم محرصاً أم متدخلأً، على أن تكون الجرائم معاقبا عليها خارج فلسطين، مع مراعاة المبادئ العامة الواردة في قانون العقوبات النافذ . 2 . يجوز ملاحقة كل من يرتكب خارج فلسطين، إحدى الجرائم المنصوص عليها في هذا القرار بقانون في إحدى الحالات الآتية :أ. إذا ارتكبت من مواطن فلسطيني .ب. إذا ارتكبت ضد أطراف أو مصالح فلسطينية .ج. إذا ارتكبت ضد أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية محل إقامته المعتاد داخل فلسطين، أو من قبل أجنبي أو شخص عديم الجنسية وجد بالأراضي الفلسطينية، ولم تتوافر في شأنه شروط التسليم القانونية .

مادة (3)

1.تتشأ وحدة متخصصة في جهاز الشرطة وقوى الأمن من مأموري الضبط القضائي تسمى "وحدة الجرائم الإلكترونية"، وتتولى الوحدة العامة الإشراف القضائي عليها، كل في دائرة اختصاصه . 2. تتولى المحاكم النظامية والوحدة العامة، وفقاً لاختصاصاتهما، النظر في دعاوى الجرائم الإلكترونية .

مادة (4)

1. كل من دخل عمداً دون وجه حق بأي وسيلة موقعا إلكترونياً أو نظاماً أو شبكة إلكترونية أو وسيلة تكنولوجيا معلومات أو جزء منها أو تجاوز الدخول المصرح به أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2 . إذا ارتكب الفعل المذكور في الفقرة (1) من هذه المادة، على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألفي دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3 . إذا ترتب على الدخول إلغاء بيانات أو معلومات إلكترونية مخزنة في النظام المعلوماتي أو حذفها أو إضافتها أو إفشاؤها أو إتلافها أو تغييرها أو نقلها أو نقاطها أو نسخها أو نشرها أو إعادة نشرها أو ألحق ضرراً بالمستخدمين أو المستفيدين، أو تغيير الموقع الإلكتروني أو

إلغائه أو تعديل محتوياته أو شغل عنوانه أو تصميماته أو طريقة استخدامه، أو انتحال شخصية مالكه أو القائم على إدارته، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.4 . إذا ارتكب الفعل المذكور في الفقرة (3) من هذه المادة على البيانات الحكومية، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (5)

كل من أعاق أو عطل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (6)

كل من أنتج أو أدخل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها أو إتلاف البرامج أو حذفها أو تعديلها، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (7)

كل من التقط ما هو مرسل عن طريق الشبكة أو إحدى وسائل تكنولوجيا المعلومات أو سجله أو اعترضه أو تتصت عمداً دون وجه حق، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (8)

1. كل من قام عمداً بفك بيانات مشفرة في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.2 . كل من استعمل بصفة غير مشروعة عناصر تشفير شخصية أو أداة إنشاء التوقيع الإلكتروني المتعلقة بتوقيع شخص غيره، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة

آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.3 . كل من ارتكب جريمة باستخدام أي من الوسائل المذكورة في الفقرة (2) من هذه المادة، يعاقب بالسجن وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (9)

1. كل من ينتفع دون وجه حق بخدمات الاتصال عن طريق إحدى وسائل تكنولوجيا المعلومات أو ما في حكمها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.2 . إذا كان الانتفاع في الفقرة (1) من هذه المادة بقصد الربح، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (10)

كل من قام عمداً، عبر استخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بإنشاء أو نشر شهادة غير صحيحة أو قدم بيانات غير صحيحة عن هويته إلى الجهات المختصة بموجب القوانين الخاصة بإصدار الشهادات بغرض طلب استصدار شهادة أو إلغائها أو إيقافها، يعاقب بالحبس وبغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (11)

1. كل من زور مستندا إلكتروني رسمياً من مستندات الدولة أو الهيئات أو المؤسسات العامة معترفاً به قانوناً في نظام معلوماتي، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.2 . إذا وقع التزوير، فيما عدا ذلك من المستندات، وكان من شأن ذلك إحداث ضرر، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.3 . كل من استعمل المستند المزور مع علمه بتزويره يعاقب بالعقوبة المقررة لجريمة استعمال السند المزور وفق قانون العقوبات النافذ.4 . كل من زور أو تلاعب بتوقيع أو أداة أو أنظمة توقيع إلكترونية رسمية، سواء تم ذلك باصطناعه أو إتلافه أو تعييبه أو تعديله أو تحويره، أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقة في بياناته أو معلوماته، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.5 . إذا وقع التزوير أو التلاعب فيما عدا ذلك من التوقيعات الإلكترونية المذكورة

في الفقرة (4) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 6 . كل من أنشا بيانات توقيع أو أداة نظام توقيع إلكتروني رسمي أو للهيئات أو للمؤسسات العامة لا يحق له الحصول عليه، مستخدماً في ذلك معلومات أو بيانات كاذبة أو خاطئة، أو تواطأ مع غيره في إنشاء ذلك، يعاقب بالسجن مدة لا تقل عن خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً. 7 . إذا وقع الإنشاء فيما عدا ذلك من التوقيعات الإلكترونية المذكورة في الفقرة (6) من هذه المادة، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد عن ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (12)

1. كل من استخدم الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في الوصول، دون وجه حق، إلى أرقام أو بيانات وسيلة التعامل الإلكترونية أو التلاعب فيها، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2 . كل من زور وسيلة تعامل إلكترونية بأي وسيلة كانت، أو صنع أو حاز بدون ترخيص أجهزة أو مواد تستخدم في إصدار أو تزوير بطاقة التعامل الإلكتروني، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة. 3 . كل من استخدم أو سهل استخدام وسيلة تعامل إلكترونية مزورة مع علمه بذلك أو قبل وسيلة تعامل إلكترونية غير سارية أو مزورة أو مسروقة مع علمه بذلك، يعاقب بالعقوبة ذاتها المنصوص عليها في الفقرة (1) من هذه المادة. 4 . إذا تم ارتكاب الأفعال المنصوص عليها في أحكام هذه المادة بقصد الحصول على أموال أو بيانات غيره أو ما تنتجه من خدمات، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين . 5. كل من استولى لنفسه أو لغيره على مال الغير بموجب الأحكام الواردة في هذه المادة، يعاقب بالحبس مدة لا تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (13)

كل من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في سرقة أموال أو اختلاسها، يعاقب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (14)

كلّ من استولى عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات لنفسه أو لغيره على مال منقول أو على سند أو توقيع إلكتروني أو بيانات إنشاء توقيع إلكتروني أو منظومة إنشاء توقيع إلكتروني، وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (15)

1. كلّ من استعمل الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. إذا كان التهديد بارتكاب جنائية أو بإسناد أمور خادشة للشرف أو الاعتبار، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (16)

1. كلّ من أرسل عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كلّ ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن هم فوق الثامنة عشر سنة ميلادية دون رضاه، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، ولا تزيد على سنتين، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 2. كلّ من أرسل أو نشر عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات قصداً كلّ ما هو مسموع أو مقروء أو مرئي يتضمن أعمالاً إباحية لمن لم يكمل الثامنة عشر سنة ميلادية أو تتعلق بالاستغلال الجنسيّ لهم، يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين. 3. كلّ من قام قصداً باستخدام الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات في إنشاء أو إعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر أو ترويج أنشطة أو أعمال إباحية لغايات التأثير على من لم يكمل الثامنة عشر سنة ميلادية أو من هو من ذوي الإعاقة، يعاقب بالحبس مدة لا

تقل عن سنتين، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة، أو بكلتا العقوبتين .

مادة (17)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن تنظيم نقل وزراعة الأعضاء البشرية النافذ، يعاقب كل من أنشأ موقعا أو تطبيقا أو حسابا إلكترونيا أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار في البشر أو الأعضاء البشرية أو تسهيل التعامل فيه، بالسجن مدة لا تزيد على سبع سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (18)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة غسل الأموال وتمويل الإرهاب النافذ، يعاقب كل من أنشأ موقعا أو تطبيقا أو حسابا إلكترونيا أو إحدى وسائل تكنولوجيا المعلومات بقصد 1. القيام بارتكاب جريمة غسل الأموال بالحسب مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين 2. القيام بارتكاب جريمة تمويل الإرهاب بالسجن أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (19)

دون الإخلال بالأحكام الواردة في القرار بقانون بشأن مكافحة المخدرات والمؤثرات العقلية النافذ، يعاقب كل من أنشأ أو نشر موقعا على الشبكة الإلكترونية، أو إحدى وسائل تكنولوجيا المعلومات، بقصد الاتجار أو الترويج للمخدرات أو المؤثرات العقلية، أو ما في حكمها، أو سهل التعامل فيها، أو بيع أو شرح أو عرض طرق إنتاج المواد المخدرة، بالسجن مدة لا تقل عن عشر سنوات، أو بغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (20)

كل من انتهك حق من حقوق الملكية الفكرية أو الأدبية أو الصناعية وفقا للتشريعات النافذة، عن طريق الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، يعاقب بالحسب مدة لا تزيد على ستة أشهر، أو بغرامة لا تقل

عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بـكلتا العقوبتين .

مادة (21)

1. لكل إنسان حق التعبير عن رأيه بالقول أو الكتابة أو التصوير أو غير ذلك من وسائل التعبير والنشر وفقاً للقانون . 2. حرية الإبداع الفني والأدبي مكفولة، ولا يجوز رفع أو تحريك الدعاوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضدّ مبدعيها إلا بأمر قضائي، ولا توقع عقوبة سالبة للحرية أو التوقيف الاحتياطي في الجرائم التي ترتكب بسبب علانية المنتج الفني أو الأدبي أو الفكري . 3. حرية الصحافة والطباعة والنشر الورقي والمرئي والمسموع والإلكتروني مكفولة، وللـفلسطينيين من أشخاص طبيعية أو اعتبارية عامة أو خاصة، حق ملكية وإصدار الصحف، وإنشاء وسائل الإعلام المرئية والمسموعة ووسائل الإعلام الرقمي وفقاً للقانون . 4. لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي .

مادة (22)

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

مادة (23)

كل من أنشأ موقعا أو تطبيقاً أو حساباً إلكترونياً أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد إدارة مشروع مقامرة أو تسهيله أو تشجيعه أو الترويج له أو عرض ألعاب مقامرة، يعاقب بالحبس مدة لا تقل عن ستة أشهر، أو بغرامة لا تقل عن خمسمائة دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بـكلتا العقوبتين .

مادة (24)

كل من أنشا موقعا أو تطبيقا أو حسابا إلكترونيا أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، بقصد عرض أي كلمات مكتوبة أو سلوكيات من شأنها أن تؤدي إلى إثارة الكراهية العنصرية أو الدينية أو التمييز العنصري بحق فئة معينة بسبب انتمائها العرقي أو المذهبي أو اللون أو الشكل أو بسبب الإعاقة، يعاقب بالحبس مدة لا تزيد عن سنة، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (25)

كل من أنشا موقعا أو تطبيقا أو حسابا إلكترونيا أو نشر معلومات على الشبكة الإلكترونية أو إحدى وسائل تكنولوجيا المعلومات، من شأنه التشويه أو التبرير لأعمال إبادة جماعية أو جرائم ضد الإنسانية نصت عليها المواثيق والقوانين الدولية أو المساعدة قسداً أو التحريض على ارتكاب جرائم ضد الإنسانية، يعاقب بالسجن مدة لا تقل عن عشر سنوات .

مادة (26)

كل من حاز بغرض الاستخدام جهازا أو برنامجا أو أي بيانات إلكترونية معدة أو كلمة سر أو ترميز دخول أو قدمها أو أنتجها أو وزعها أو استوردها أو صدرها أو روج لها، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بالسجن مدة لا تزيد على خمس سنوات، وبغرامة لا تقل عن ثلاثة آلاف دينار أردني، ولا تزيد على خمسة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً .

مادة (27)

1. كلّ موظف ارتكب أيًا من الجرائم المنصوص عليها في هذا القرار بقانون، مستغلاّ صلاحياته وسلطاته أثناء تأدية عمله، أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلث. 2. كلّ من ارتكب، من موظفي مزودي الخدمة، أيًا من الجرائم المنصوص عليها في هذا القرار بقانون، أثناء تأدية عمله أو بسببه أو سهل ذلك لغيره، تزيد العقوبة بمقدار الثلثين .

مادة (28)

كل من حرض أو ساعد أو اتفق مع غيره على ارتكاب جريمة من الجرائم المنصوص عليها بموجب أحكام هذا القرار بقانون، بأي وسيلة إلكترونية، ووقعت الجريمة بناءً على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبات المقررة لفاعلها الأصلي .

مادة (29)

إذا ارتكب، باسم الشخص المعنوي أو لحسابه، إحدى الجرائم المنصوص عليها في هذا القرار بقانون، يعاقب بغرامة لا تقل عن خمسة آلاف دينار أردني، ولا تزيد على عشرة آلاف دينار أردني، وللمحكمة أن تقضي بحرمان الشخص المعنوي من مباشرة نشاطه لمدة أقصاها خمس سنوات أو أن تقضي بحله في حال كانت الجريمة معاقب عليها بالحبس لمدة لا تقل عن سنة، وذلك مع عدم الإخلال بالمسؤولية الجنائية للشخص الطبيعي التابع له .

مادة (30)

كل من نشر قصدا معلومات عن موقع إلكتروني محجوب بموجب أحكام المادة (39) من هذا القرار بقانون، باستخدام أنظمة أو موقع أو تطبيق إلكتروني، يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين .

مادة (31)

يلتزم مزود الخدمة، وفقا للإجراءات القانونية المقررة بالآتي 1. تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب الوحدة أو المحكمة المختصة 2. حجب رابط أو محتوى أو تطبيق على الشبكة الإلكترونية بناءً على الأوامر الصادرة إليها من الجهات القضائية، مع مراعاة الإجراءات الواردة في المادة (39) من هذا القرار بقانون 3. الاحتفاظ بمعلومات المشترك لمدة لا تقل عن ثلاث سنوات لغايات ما ورد في الفقرة (1) من هذه المادة 4. التعاون ومساعدة الجهات المختصة وبناءً على قرار قاضي المحكمة المختصة في جمع أو تسجيل المعلومات أو البيانات الإلكترونية والاحتفاظ المؤقت بها .

مادة (32)

1. للوحدة العامة أو من تنتدبه من مأموري الضبط القضائي تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة 2. يجب أن يكون أمر التفتيش مسبباً ومحددًا، ويجوز تجديده أكثر من مرة، ما دامت مبررات هذا الإجراء قائمة 3. إذا أسفر التفتيش في الفقرة (2) من هذه المادة، عن ضبط أجهزة أو أدوات

أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات، وعرضها على الوحدة العامة لاتخاذ ما يلزم بشأنها. 4. لوكيل الوحدة أن يأذن بالنفاذ المباشر لمأموري الضبط القضائي أو من يستعينون بهم من أهل الخبرة إلى أي وسيلة من وسائل تكنولوجيا المعلومات، وإجراء التفتيش فيها بقصد الحصول على البيانات أو المعلومات. 5. يشترط في مأمور الضبط القضائي أن يكون مؤهلا للتعامل مع الطبيعة الخاصة للجرائم الإلكترونية .

مادة (33)

1. للوحدة العامة الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات أو المعلومات الإلكترونية أو بيانات المرور أو البيانات المتعلقة بحركة الاتصالات أو بمستعملها أو معلومات المشترك ذات الصلة بالجريمة الإلكترونية. 2. للوحدة العامة الإذن بالضبط والتحفظ على كامل نظام المعلومات أو جزء منه أو أي وسيلة من وسائل تكنولوجيا المعلومات التي من شأنها أن تساعد على كشف الحقيقة. 3. إذا لم يكن الضبط والتحفظ على نظام المعلومات ضروريا أو تعذر إجراؤه، تتسخ البيانات أو المعلومات التي لها علاقة بالجريمة والبيانات التي تؤمن قراءتها وفهمها على وسيلة من وسائل تكنولوجيا المعلومات. 4. إذا استحال إجراء الضبط والتحفظ بصفة فعلية، يتعين حفاظا على أدلة الجريمة استعمال كافة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزنة بنظام المعلومات. 5. تتخذ الاحتياطات الضرورية للحفاظ على سلامة المضبوط المتحفظ عليه، بما في ذلك الوسائل الفنية لحماية محتواها. 6. تحرر قدر الإمكان قائمة بالمضبوط المتحفظ عليه بحضور المتهم أو من وجد لديه المضبوط المتحفظ عليه، ويحرر تقرير بذلك، ويحفظ المضبوط المتحفظ عليه حسب الحالة في ظرف أو مغلف مختوم، ويكتب عليه ورقة مع بيان تاريخ التحفظ وساعته وعدد المحاضر والقضية .

مادة (34)

1. لقاضي الصلح أن يأذن للنائب العام أو أحد مساعديه بمراقبة الاتصالات والمحادثات الإلكترونية، وتسجيلها، والتعامل معها للبحث عن الدليل المتعلق بجناية أو جنحة يعاقب عليها بالحبس مدة لا تقل عن سنة، وذلك لمدة خمسة عشر يوما قابلة للتجديد لمرة واحدة، بناءً على توافر دلائل جدية، وعلى من قام بالتفتيش أو المراقبة أو التسجيل أن ينظم محضرا بذلك يقدمه إلى الوحدة العامة. 2. للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأي بيانات، بما فيها حركة الاتصالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المشترك التي يراها لازمة لمصلحة التحقيقات لغايات الفقرة (1) من هذه المادة، باستعمال الوسائل الفنية المناسبة، والاستعانة بذلك عند الاقتضاء بمزودي الخدمات، حسب نوع الخدمة التي يقدمها .

مادة (35)

على الجهات المختصة اتخاذ التدابير والإجراءات الكفيلة بالحفاظ على سلامة الأجهزة أو الأدوات أو وسائل تكنولوجيا المعلومات أو الأنظمة الإلكترونية أو البيانات أو المعلومات الإلكترونية وخصوصيتها محل التحفظ، إلى حين صدور قرار من الجهات القضائية ذات العلاقة بشأنها .

مادة (36)

1. للمحكمة المختصة أن تأذن بالاعتراض الفوري لمحتوى اتصالات، وتسجيلها أو نسخها بناءً على طلب من قبل النائب العام أو أحد مساعديه، ويتضمن قرار المحكمة جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له، ومدته 2. تكون مدة الاعتراض في الفقرة (1) من هذه المادة، لا تزيد على ثلاثة أشهر من بداية تاريخ الشروع الفعلي في إنجازه، قابلة للتمديد مرة واحدة فقط 3. يتعين على الجهة المكلفة بتنفيذ إذن الاعتراض إعلام الوحدة العامة بالتاريخ الفعلي لانطلاق عملية الاعتراض، والتنسيق معها بخصوص اتخاذ التدابير اللازمة لحسن سيرها .

مادة (37)

يعتبر الدليل الناتج بأي وسيلة من وسائل تكنولوجيا المعلومات أو أنظمة المعلومات أو شبكات المعلومات أو المواقع الإلكترونية أو البيانات والمعلومات الإلكترونية من أدلة الإثبات .

مادة (38)

تعتبر الأدلة المتحصل عليها بمعرفة الجهة المختصة أو جهات التحقيق من دول أخرى، من أدلة الإثبات، طالما أن الحصول عليها قد تمّ وفقا للإجراءات القانونية والقضائية للتعاون الدولي .

مادة (39)

1. الجهات التحري والضبط المختصة، إذا ما رصدت قيام مواقع إلكترونية مستضافة داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو غيرها، من شأنها تهديد الأمن القومي أو النظام العام أو الآداب العامة، أن تعرض محضرا بذلك على النائب العام أو أحد مساعديه، وتطلب الإذن بحجب الموقع أو المواقع الإلكترونية أو حجب بعض روابطها من العرض 2. يقدم النائب العام أو أحد مساعديه طلب الإذن لمحكمة الصلح خلال (24 ساعة)، مشفوعا بمذكرة برأيه، وتصدر المحكمة قرارها في الطلب، في ذات يوم

عرضه عليها إما بالقبول أو بالرفض، على ألا تزيد مدة الحجب على ستة أشهر، ما لم تجدد المدة وفقاً للإجراءات المنصوص عليها في هذه المادة .

مادة (40)

فيما عدا الالتزامات المهنية المنصوص عليها في القانون، لا يجوز الاستناد إلى أسرار المهنة أو مقتضياتها للامتناع عن تقديم المعلومات أو الوثائق التي تطلب وفقاً لأحكام القانون .

مادة (41)

تلتزم أجهزة الدولة ومؤسساتها وهيئاتها والجهات والشركات التابعة لها بالآتي 1. اتخاذ التدابير الأمنية الوقائية اللازمة لحماية أنظمتها المعلوماتية، ومواقعها الإلكترونية، وشبكات المعلوماتية، والبيانات والمعلومات الإلكترونية الخاصة بها 2. الإسراع في إبلاغ الجهة المختصة عن أي جريمة منصوص عليها في هذا القرار بقانون، فور اكتشافها أو اكتشاف أي محاولة للاختراق أو الاعتراض أو التنصت بشكل غير مشروع، وتزويد الجهة المختصة بجميع المعلومات لكشف الحقيقة 3. الاحتفاظ ببيانات تكنولوجيا المعلومات، ومعلومات المشترك لمدة لا تقل عن (120) يوماً، وتزويد الجهة المختصة بتلك البيانات 4. التعاون مع الجهة المختصة لتنفيذ اختصاصاتها .

مادة (42)

1. تعمل الجهات المختصة على تيسير التعاون مع نظيراتها في البلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها، أو طبق مبدأ المعاملة بالمثل، بقصد الإسراع في تبادل المعلومات، بما من شأنه أن يكفل الإنذار المبكر بجرائم أنظمة المعلومات والاتصال، ونفاذي ارتكابها، والمساعدة على التحقيق فيها، وتتبع مرتكبيها 2. يتوقف التعاون المشار إليه في الفقرة السابقة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها، والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القرار بقانون .

مادة (43)

1. يتعين على الجهات المختصة أن تقدم العون للجهات النظيرة في الدول الأخرى، لأغراض تقديم المساعدة القانونية المتبادلة، وتسليم المجرمين في التحقيقات والإجراءات الجنائية المرتبطة بالجرائم المنصوص عليها في هذا القرار بقانون، وفقاً للقواعد التي يقرها قانون الإجراءات الجزائية النافذ والاتفاقيات الثنائية أو متعددة الأطراف التي تكون الدولة طرفاً فيها، أو بمبدأ المعاملة بالمثل، وذلك بما لا يتعارض مع أحكام هذا القرار بقانون أو أي قانون آخر. 2. لا ينفذ طلب المساعدة القانونية أو طلب تسليم المجرمين، استناداً إلى أحكام هذا القرار بقانون، إلا إذا كانت قوانين الدولة الطالبة وقوانين الدولة تعاقب على الجريمة موضوع الطلب أو على جريمة مماثلة، وتعتبر ازدواجية التجريم مستوفاة، بغض النظر عما إذا كانت قوانين الدولة الطالبة تدرج الجريمة في فئة الجرائم ذاتها أو تستخدم في تسمية الجريمة المصطلح ذاته المستخدم في الدولة، بشرط أن يكون الفعل موضوع الطلب مجرماً بمقتضى قوانين الدولة الطالبة.

مادة (44)

مع عدم الإخلال بأي عقوبة أشد، ينص عليها قانون العقوبات الساري أو أي قانون آخر، يعاقب مرتكبو الجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات المنصوص عليها فيه.

مادة (45)

كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الإلكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، يعاقب بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع.

مادة (46)

كل من أفشى سرية الإجراءات المنصوص عليها في هذا القرار بقانون، في غير الأحوال المصرح بها قانوناً، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني، ولا تزيد على ألف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً، أو بكلتا العقوبتين.

مادة (47) كل من أقدم على العبث بأدلة قضائية معلوماتية أو أقدم على إتلافها أو إخفائها أو التعديل فيها أو محوها، يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن ألف دينار أردني، ولا تزيد على ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة قانوناً.

مادة (48)

يعاقب من يشترك بطريق الاتفاق أو التحريض أو المساعدة أو التدخل في ارتكاب جناية أو جنحة معاقب عليها بموجب أحكام هذا القرار بقانون، بالعقوبات ذاتها المقررة للفاعل الأصلي، وإن لم تقع الجريمة يعاقب بنصف العقوبة .

مادة (49)

يعد مرتكبا جريمة الشروع كلّ من شرع في ارتكاب جناية أو جنحة من الجرائم المنصوص عليها في هذا القرار بقانون، ويعاقب بنصف العقوبة المقررة لها .

مادة (50)

دون الإخلال بالعقوبات المنصوص عليها في هذا القرار بقانون، وحقوق الغير حسن النية، على المحكمة أن تصدر قرارا يتضمن الآتي .1:مدة إغلاق المحل، وحجب الموقع الإلكتروني الذي ارتكبت فيه أو بواسطته تلك الجرائم بحسب الأحوال .2. مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القرار بقانون أو الأموال المتحصلة منها، على أن تكون إزالة المخالفة على نفقة الفاعل .

مادة (51)

تضاعف العقوبة المنصوص عليها في هذا القرار بقانون في حال تكرار الجاني أيا من الجرائم المنصوص عليها فيه، سواء ارتكبت في فلسطين أو خارجها، وتعتبر الأحكام الأجنبية سابقة في التكرار بحق الجاني .

مادة (52)

تضاعف العقوبة المقررة للجرائم المعاقب عليها بموجب أحكام هذا القرار بقانون، في أي من الحالات الآتية.1 : إذا وقعت الجريمة على موقع أو نظام معلوماتي أو بيانات أو أرقام أو حروف أو شفرات أو صور يدار بمعرفة الدولة أو أحد الأشخاص المعنوية العامة أو مملوك لها أو يخصها، بما في ذلك الهيئات المحلية .2. ارتكاب الجاني الجريمة من خلال عصابة منظمة .3. التغرير أو استغلال من لم يكمل الثامنة عشر سنة ميلادية.4 . إذا وقعت الجريمة على نظام معلومات أو موقع إلكتروني أو شبكة معلوماتية تتعلق بتحويل الأموال أو بتقديم خدمات الدفع أو التقاص أو التسويات أو أي من الخدمات المصرفية المقدمة من البنوك والشركات المالية .

مادة (53)

يعفى من العقوبات المنصوص عليها في هذا القرار بقانون، كلّ من بادر من الجناة بإبلاغ السلطات المختصة بأي معلومات عن الجريمة وعن الأشخاص المشتركين فيها، وذلك قبل علم السلطات بها وقبل وقوع الضرر، ويجوز للمحكمة أن تقضي بوقف تنفيذ العقوبة إذا حصل الإبلاغ بعد علم السلطات المختصة، وأدى إلى ضبط باقي الجناة .

مادة (54)

تتولى الوزارة وفقا لاختصاصها تقديم الدعم والمساعدة الفنية لجهات إنفاذ القانون، ويعتبر موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون .

مادة (55)

1.يلغى القرار بقانون رقم (16) لسنة 2017م، بشأن الجرائم الإلكترونية .2.يلغى كلّ ما يتعارض مع أحكام هذا القرار بقانون .

مادة (56)

يعرض هذا القرار بقانون على المجلس التشريعي في أول جلسة يعقدها لإقراره .

مادة (57)

على الجهات المختصة كافة، كلّ فيما يخصه، تنفيذ أحكام هذا القرار بقانون، ويعمل به من تاريخ نشره في الجريدة الرسمية .

صدر في مدينة رام الله بتاريخ: 2018/04/29 ميلادية الموافق: 13/شعبان/1439 هجرية محمود عباس رئيس دولة فلسطين رئيس اللجنة التنفيذية لمنظمة التحرير الفلسطينية.

ملحق (8) مذكرة قانونية حول القرار بقانون رقم (10) لسنة 2018 فيما يخص الجرائم الإلكترونية:



الهيئة المستقلة لحقوق الإنسان
ديوان المظالم
The Independent Commission for Human Rights



20/5/2018

مذكرة قانونية

حول القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية

اتطالفاً من دورها المسند إليها في القانون الأساسي المعدل لسنة 2003 وتعديلاته، وفي المرسوم الرئاسي رقم (59) لسنة 1994، في تعزيز منظومة حقوق الإنسان في دولة فلسطين، وفي الرقابة على السياسات والتشريعات الوطنية، لضمان انسجامها مع القانون الأساسي، ومع الاتفاقيات الدولية لحقوق الإنسان التي انضمت إليها دولة فلسطين. تابعت الهيئة المستقلة لحقوق الإنسان "ديوان المظالم"، عن كثب كافة الأحداث والإجراءات وردود الأفعال التي أعقبت صدور القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية الصادر في تموز/ يوليو من العام 2017، وقد عبرت الهيئة حينها عن خشيتها وقلقها البالغ من القرار بقانون المذكور، لما تضمنه من أحكام ما من شأنه أن تشكل تهديداً خطيراً للحق في حرية الرأي والتعبير والحق في الخصوصية وحرمة الحياة الخاصة للمواطنين، مطالباً ومعهها مؤسسات المجتمع المدني، بالعمل على تعديله بما يعزز من حقوق المواطنين وحررياتهم الأساسية وبما ينسجم مع القانون الأساسي ومع التزامات دولة فلسطين على الصعيد الدولي. وقد شاركت الهيئة في هذا السياق، في العديد من جلسات الحوار مع الجهات الرسمية بهدف الوصول إلى تعديلات جوهرية على القرار بقانون المذكور على نحو يوازن بين مكافحة الجرائم الإلكترونية وحماية الحقوق والحرريات الأساسية للمواطنين.

وإذ تعبر الهيئة مجدداً عن تقديرها لافتتاح الجهات الرسمية على الحوار معها ومع مؤسسات المجتمع المدني حول القرار بقانون المذكور، وإذ ترحب بالاستجابة التي عدد من توصياته وبخاصة إلغاء النصوص العامة والفضفاضة بشكل صريح في القانون الجديد، وتخفيف الجزاءات الجنائية بشكل واضح، والتي كانت أحد أبرز أسباب اعتراض الهيئة ومؤسسات المجتمع المدني على القرار بقانون السابق، إلا أن الهيئة المستقلة في ذات الوقت، وانطلاقاً من دورها المشار إليه أعلاه، ومن المسؤولية التي تحملها في هذا السياق، ترغب في أن تضع أمام الرأي العام الفلسطيني مجموعة من الملاحظات على القرار بقانون الجديد، والتي سبق أن أرسلتها إلى الحكومة في سياق إبداء ملاحظاتها على هذا القرار بقانون عندما كان في طور المشروع، وهي تأسف لعدم الأخذ بها كما ظهر من النسخة المنشورة في الوقائع الفلسطينية. وإذ تنشر الهيئة هذه الملاحظات للجمهور، فإن تأمل بالاستجابة إليها، تعزيزاً لحقوق وحرريات المواطنين، وتطبيقاً لالتزامات دولة فلسطين في الاتفاقيات الدولية لحقوق الإنسان، وهي تعبر عن استنادها للحوار مع الجهات الرسمية المختصة للوصول إلى قانون عصري للجرائم الإلكترونية يحمي حقوق الإنسان وحرياته الأساسية.

أمانة الهيئة المستقلة لحقوق الإنسان بموجب مرسوم رئاسي رقم (59) عام 1993، والمادة (31) من القانون الأساسي المعدل الفلسطيني لعام 2003

المقر الرئيسي - مكتب الوسط - رام الله : هاتفه 2986958 / 2960241 / 2987536 2 972 ، ص.ب. 2264 ، فلسطين : 2987211 2 972

مكتب الشمال : هاتفه 2335668 9 972 ، فاكس : 97292366408

مكتب الجنوب : هاتفه 2750549 2 972 ، فاكس : 0097222295443 ، 00972222746885 / 0097222211120

مكتب غزة : هاتفه 0097282821438 ، فاكس : 0097282815019

Email: ichr@ichr.ps

Web Page: www.ichr.ps

وفي الأتي تبرز الملاحظات الجوهرية على أحكام القرار بقانون المنكور، والتي يترتب على عدم إعادة النظر أو الالتفات عنها، أن يكون القرار بقانون منطوياً على انتهاكات خطيرة لحقوق الإنسان وحرياته الأساسية. مع التأكيد هنا، على تحفظ الهيئة الدائم بالاستمرار والتوسع في إصدار قرارات لها قوة القانون في ظل غياب المجلس التشريعي.

مرة أخرى ينص القرار بقانون بشأن الجرائم الالكترونية على سريانه من تاريخ نشره في الجريد الرسمية (مادة 57)، دون أن يعطي مدة كافية للجمهور ولجهات إنفاذ القانون بدراسته، وهذا يناقض ما تسيّر عليه القوانين الجنائية القديمة والحديثة، التي يُنص فيها على أن سريانه يكون بعد فترة من الزمن لا تقل عن شهر، حتى يتسّن للمخاطبين بأحكامها معرفة حقوقهم وواجباتهم وتقييم سلوكهم بالبناء عليها، وبغير ذلك، يكون القانون مخالف لمبدأ الشرعية الجنائية وللحق في العلم بالقاعدة القانونية التي نص عليها القانون الأساسي في المادة (15) منه.

بالرغم من أن القرار بقانون الجديد يتقدم عن القرار بقانون الحالي بإلغائه للنصوص المجرمة لحرية الرأي والتعبير بمصطلحات عامة وفضفاضة مثل النظام العام والآداب العامة والأمن القومي والسلام الأهلي...، إلا أن الهيئة ترى بأنه قد جرى فتح الباب مجدداً لتجريم الأفعال والكتابات المنضوية تحت مظلة حرية الرأي والتعبير بموجب مصطلحات عامة وفضفاضة، وذلك من خلال نص المادة (45) من القرار بقانون، والتي تعاقب كل من ارتكب فعلاً يشكل جريمة بموجب أي تشريع نافذ باستخدام الشبكة الالكترونية أو بإحدى وسائل تكنولوجيا المعلومات، أو اشترك فيها أو تدخل فيها أو حرض على ارتكابها، ولم ينص عليها في هذا القرار بقانون، بالعقوبة ذاتها المقررة لتلك الجريمة في ذلك التشريع. وذلك يعني فتح المجال لتطبيق نصوص قانون العقوبات وقانون المطبوعات والنشر ساربي المفعول، واللذين يتضمنان تجريماً لكتابات وأقوال تدخل ضمن حرية الرأي والتعبير بموجب مصطلحات عامة وفضفاضة، مثل جرائم الذم والقلم وإطالة اللسان وقذح المقامات العليا وإثارة النزعات العنصرية والطائفية، وهي نصوص عليها ملاحظات كثيرة، من حيث عدم انسجامها مع مبدأ الشرعية الجنائية وحرية الرأي والتعبير، وقد استخدمت هذه النصوص لقمع حرية الرأي والتعبير وحبس المواطنين والصحفيين والناشطين، حسباً احتياطياً، بل ومحاكمتهم جنائياً. إضافة إلى ذلك، فإن التعليق العام رقم (34) للجنة المعنية بحقوق الإنسان في الأمم المتحدة، والاتجاه الدولي الحديث، يذهب إلى إلغاء صفة التجريم عن "جرائم" الذم والقذح، والاكتفاء باعتبارها أفعال ضارة تستلزم التعويض المدني في حالة مطالبة المتضرر بذلك، والذي شددت تلك المعايير بالنسبة للمتضرر على التفرقة -حتى في ظل المطالبة المدنية- بين إذا ما كان شخصية عامة أو فرد عادي، واعتبرت أن ذم الشخصية العامة أو قذحها فيما يتصل بعملها العام لا يخضع للتعويض المدني. وعلى ذلك، فإن الهيئة تطالب بإلغاء نص المادة (45) كلياً، والعمل على تعديل نصوص قانون العقوبات وقانون المطبوعات والنشر بما يؤدي إلى إلغاء النصوص المجرمة فيهما لأفعال وأقوال وكتابات تعتبر من ضمن حرية الرأي والتعبير على النحو المشار إليه أعلاه.

تضمن القرار بقانون العديد من النصوص المجرمة لعدد من الأفعال على أساس توقع الخطر فقط، ومجرد القصد -الذي يصار البحث فيه بعد تحقق الضرر-، وليس على أساس وقوع الضرر، الأمر الذي يدخل كثير من الأفعال في دائرة التجريم بالرغم من عدم وجود أي ضرر يكون قد نجم عنها، وقد تشكل هذه النصوص بصيغتها الحالية تهديداً لحرية الرأي والتعبير، وتقييداً لاستخدام شبكة الانترنت، وتوسعاً غير مبرراً في التجريم. وبالتالي، فإننا نطالب بتعديل صياغة هذه النصوص على نحو يجعلها من جرائم الضرر وليس الخطر، بما يعني عدم الاكتفاء بالقصد وتوقع الخطر للتجريم

والعقاب، بل اشتراط وقوع الضرر لتجريمها. وهذه النصوص هي: المادة (6)، المادة (11) فقرة 2 و4)، المواد (17 - 19)، المواد (22 - 26).

تتظر الهيئة بإيجابية إلى نص المادة (21) من القرار بقانون، والذي أكد على حريات دستورية، وأظهر حسن نوايا القرار بقانون وتقدمه عن سابقه، إلا أننا نرى أن المكان الصحيح لهذه المادة يكون ضمن المبادئ العامة للقرار بقانون، والتي ترد عادة في مطلع التشريع. ويمكن في هذا السياق، ومحل ترحيب بالنسبة لنا، أن يتم وضع نص في المبادئ العامة بجوار نص المادة (21) المذكور، ينص على حظر تقييد أي نص في هذا القرار بقانون على نحو يتعارض مع الحقوق والحريات المكفولة في القانون الأساسي أو في الاتفاقيات الدولية لحقوق الإنسان. وبالعودة إلى مضمون المادة (21) فإننا نرى أيضاً أن الفقرة الثانية منها والتي نظمت موضوع رفع أو تحريك الدعوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضد مبدعيها، قد انتقصت من ضمانات مهمة لهذا الموضوع، بجعلها صلاحية رفع الدعوى أو تحريكها.... بأمر قضائي، وليس بموجب حكم قضائي، فالمصادرة لا تتم إلا بموجب حكم قضائي صادر عن محكمة مختصة، لذا نوصي بتعديل هذه المادة بالنص على أن مصادرة الأعمال الفنية والأدبية والفكرية لا تجوز إلا بحكم قضائي صادر عن محكمة مختصة.

بالرغم من حظر القرار بقانون في المادة (1/22) منه، التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته، إلا أنه لا يضع عقوبة على مثل هذا التدخل الخطير، وبخاصة أن التدخل التعسفي أو غير القانوني يأتي دائماً من جهة الإدارة، وعلى ذلك نوصي بتعديل هذه المادة ببيان العقوبة المناسبة على هذا التدخل والنص على عدم تقادم هذه الجريمة، انسجاماً في ذلك مع المادة (32) من القانون الأساسي. أما بالنسبة للفقرة الثانية من ذات المادة، والتي جرمت إنشاء موقعاً أو تطبيقاً أو حساباً إلكترونياً.... بقصد نشر أخباراً أو صوراً أو تسجيلات صوتية أو مرئية... تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة، فإنه من الملاحظ عليها التوسع في التجريم، إذ اعتمدت على القصد دون اشتراط وقوع الضرر، فمجرد إنشاء الموقع أو التطبيق بقصد نشر الأخبار أو الصورة المتصلة بالتدخل غير القانوني، كافي، حتى لو لم يتم استخدام الموقع أو وقوع ضرر. كما أن هذه الفقرة لم تربط الملاحقة الجنائية بشكوى الفريق المتضرر بالرغم من ارتباطها بالحق الشخصي أكثر من ارتباطها بالحق العام. والأهم من ذلك، أن هذه المادة لا تفرق بين الشخصية المستهدفة من التدخل، فيما إذا كانت شخصية عامة أو فرد عادي، فالتدخل في حياة الشخصية العامة من خلال نشر الصور أو المعلومات الخاصة أو العائلية مباحة إذا كانت تتعلق بالعمل العام لتلك الشخصية. وعلى ذلك، نوصي بتعديل هذه الفقرة بصياغتها على نحو يجعلها من جرائم الضرر وليس الخطر، وربط الملاحقة الجنائية فيها على شكوى الفريق المتضرر، وتفريقها بين التدخل في حياة الشخصية العامة وحياة الشخص العادي، وهنا يلزم أفراد القرار بقانون تعريف للشخصية العامة.

تمنح المادة (29) من القرار بقانون المحكمة صلاحية القضاء حل الشخص المعنوي إذا ارتكب باسمه أو لحسابه إحدى الجرائم المنصوص عليها في هذا القرار بقانون، إذ إن عقوبة الحل وإن كان توقيعها من صلاحية للمحكمة بموجب حكم نهائي، فإنها من العقوبات القاسية، وهنا بالتحديد يمكن أن توقع على أي جريمة حتى لو كانت جنحة بسيطة، مما يعني عدم وجود تناسب بين العقوبة والجريمة، هذا بالإضافة إلى الآثار الاقتصادية التي يمكن أن تتركها عقوبة الحل على موظفي الشخص المعنوي. وسيكون من الأفضل في هذا السياق، تحديد الجرائم التي يمكن للمحكمة أن تلجأ فيها إلى حل الشخص المعنوي، والتي يجب أن تكون من الجنایات أو الجرائم الخطيرة، ويمكن في هذا السياق، الاستناد إلى نص

المادة (36) من قانون العقوبات التي تحدد مبررات وقف الهيئات الاعتبارية، وهي حالات اقتراف مديرها أو أعضاء إدارتها... باسمها أو بإحدى وسائلها جنائية أو جنحة مقصودة يعاقب عليها بمسئتي حبس على الأقل.

حددت المادة (31) من القرار بقانون التزامات مزود الخدمة، وجاء في فقرتها الأولى "تزويد الجهات المختصة بمعلومات المشترك التي تساعد في كشف الحقيقة، بناءً على طلب النيابة أو المحكمة المختصة. ونرى في هذا السياق، أن عبارة "التي تساعد في كشف الحقيقة" قد تتضمن الوصول إلى معلومات المحتوى التي يخضع الحصول عليها لإجراءات مشددة وليس فقط بناءً على طلب النيابة أو المحكمة المختصة، ولذا نوصي باقتصار الفقرة على الالتزام بتزويد الجهات المختصة بمعلومات المشترك المعرفة بالمادة الأولى من القرار بقانون.

لقد جاء نص المادة (1/34) من القرار بقانون، والتي تنظم حالات مراقبة الاتصالات والمحادثات الإلكترونية، منسجماً مع نص المادة (51) من قانون الإجراءات الجزائية ساري المفعول، إلا أن الفقرة الثانية من ذات المادة، جاءت مخالفة لنص المادة (51) المذكور أعلاه، ومنقصة بشكل واضح من ضمانات مراقبة الاتصالات، بإسقاطها لشرط الحصول على إذن قاضي الصلح بالجمع والتزويد الفوري للبيانات بما فيها بيانات المرور. وإسقاطها لشرط جسامه الجريمة، بأن تكون جنائية أو جنحة لا تقل عقوبتها عن الحبس مدة سنة، وعلى ذلك، نوصي بتعديل الفقرة الثانية بمقارنتها مع الفقرة الأولى والمادة (51) من قانون الإجراءات المذكورة أعلاه، وبخاصة، كونها تمنح السلطات الحصول على بيانات المرور، وهي بيانات يجب أن تحاط بضمانات مشددة، حتى أن هناك اتجاه يجعل من الحصول على بيانات المرور بمثابة إدانة الذات، وهو أمر محظور في المعايير الدولية.

المواد (32: 33) من القرار بقانون تمنح النيابة العامة أو من تقتنيه من مأموري الضبط القضائي صلاحية تفتيش الأشخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة، وصلاحية الحصول على الأجهزة أو الأدوات أو الوسائل أو البيانات... والإذن بضغطها والتحقق عليها ونسخها وتسجيلها، والاستعانة بمن يروته من أهل الخبرة. فعلاوة عن أن هذه المادة تنتقص من بعض الضمانات التي نص عليها قانون الإجراءات الجزائية من حيث عدم تحديدها مدة سريان مكررة التفتيش، وعدم اشتراطها أن يكون التفتيش بحضور المتهم، وعدم اشتراطها كذلك أن يكون التفتيش لغايات التحقيق في جريمة ارتكبت فعلاً لاستخلاص الدليل، وليس بناءً على شكوك حتى لو كانت قوية لارتكاب جريمة، فإنها أيضاً، تتعلق بتفتيش أجهزة إلكترونية وأنظمة تخزين البيانات، وهي أقرب أن تكون تفتيش لمغلفات مغلقة داخل البيت أو تفتيش في أوراق مكتبة كاملة يصعب فيها بشكل كبير فصل البيانات المتعلقة بالجريمة عن غيرها من البيانات التي يمكن الاطلاع عليها من قبل أجهزة إنفاذ القانون، وهناك من لا يعتبر هذا التفتيش تفتيش بل يعتبره ضمن مراقبة الاتصالات. وهي مع هذا الحال، يجب أن تخضع لإجراءات مراقبة الاتصالات. لذلك، وانطلاقاً من الخصوصية الحساسة التي تمنع به هذه الأجهزة والأنظمة، ومن صعوبة تصنيف البيانات التي تحتويها (تتعلق بالجريمة أم لا)، فإنه يكون من اللازم حماية للحق في الخصوصية وحرمة الحياة الخاصة للمستخدمين، أن يكون إجراء تفتيش هذه الأجهزة والأنظمة مرهون بحصول النيابة العامة على أمر صادر عن المحكمة المختصة، واشتراط أن يكون هذا التفتيش بشأن جريمة ارتكبت، إضافة إلى النص على الضمانات الأخرى التي يوفرها قانون الإجراءات الجزائية فيما يتعلق بالتفتيش.

10. تنظم المادة (39) من القرار بقانون موضوع حجب المواقع الإلكترونية، وبالرغم من أن حجب الانترنت، إجراء مدان، بحسب قرار مجلس حقوق الإنسان في الأمم المتحدة رقم (A/HRC/32/L.20) بتاريخ 2016/06/27، إلا أنه يكون مقبول في بعض الأنظمة بشرط توفر مجموعة من الضمانات لاتخاذ مثل هذا الإجراء الخطير، بأن يكون لأسباب

واضحة، وبناء على أمر صادر عن المحكمة المختصة، وأن يكون لمدة محددة، إضافة إلى إمكانية الطعن به لدى المرجع المختص. وهي ضمانات غير متوفرة في هذه المادة، لأسباب الحجب التي تسوقها عامة وفضفاضة، ويرى هنا تحديد أسباب الحجب بوضع عبارات أو صور أو أفلام أو أي مواد دعائية أو غيرها نتج عنها ضرر يترتب على أي من الجرائم المنصوص عليها في هذا القرار بقانون، بدلاً من شأنها تهديد الأمن القومي أو النظام العام...، كما أن هذه المادة لا تحدد مدة قصوى للحجب، فهي حددته بستة أشهر قابلة للتجديد دون تحديد سقف أعلى للتجديد، وهذا يعني اعتبار الحجب عقوبة بدلاً من اعتباره إجراء تحفظي. إضافة إلى أن هذه المادة لا تنص على إمكانية استئناف القرار الصادر بقبول الحجب. وعلى ذلك، نرى تعديل هذه المادة بتضمينها الضمانات المذكورة أعلاه.

11. بعض نصوص القرار بقانون تخلط ولا تفرق بين الجنائية والجنحة على نحو يفقد لأساس قانوني. فمثلاً تنص المادة (4/4) منه على أن عقوبة ارتكاب الفعل المذكور في الفقرة (3).... هي السجن مدة لا تزيد على خمس سنوات وغرامة لا تقل عن ألف دينار أردني... فالسجن هو عقوبة جنائية، بينما الغرامة عقوبة جنحوية مهما بلغت قيمتها، وبالتالي، لا يمكن وصف هذه الجريمة بأنها جنحوية ولا يمكن وصفها في ذات الوقت بأنها جنائية، الأمر الذي يشير مشكلة في اختصاص المحكمة، ويؤثر بشكل كبير على أحكام العود والتكرار التي نص عليها القرار بقانون نفسه.

12. في مخالفة صريحة للمادة (21) من قانون الإجراءات الجزائية، التي حددت الأشخاص الذين يعتبرون من الضبط القضائي، ومن ضمنهم الموظفون الذي خولو صلاحية الضبط القضائي بموجب القانون. نصت المادة (54) من القرار بقانون على أن موظفو الوزارة المعينون من قبل الوزير مأموري ضبط قضائي لغايات تنفيذ أحكام هذا القرار بقانون. وعلى ذلك، تطالب بالتحديد الدقيق للمسميات الوظيفية في وزارة الاتصالات وتكنولوجيا المعلومات التي تمتع بصفة الضبط القضائي، وبألا يكون تعيين موظفي الضبط القضائي بموجب قرار وزاري، لأن صفة الضبط القضائي لا تمنح بحسب المادة (21) فقرة 4) من قانون الإجراءات الجزائية ساري المفعول إلا بموجب القانون.

انتهى...