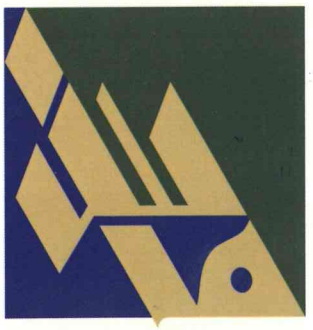

معهد أبحاث السياسات الاقتصادية (ماس)

دراسة نقدية للإطار القانوني للجرائم الإلكترونية في الأراضي الفلسطينية

2012

معهد أبحاث السياسات الاقتصادية الفلسطيني (ماس)

تأسس في القدس عام 1994 كمؤسسة مستقلة، غير ربحية متخصصة في أبحاث السياسات الاقتصادية والاجتماعية.

يوجه عمل ماس من قبل مجلس أمناء يضم شخصيات مرموقة من أكاديميين ورجال أعمال من فلسطين والدول العربية.

رسالة المعهد

معهد أبحاث السياسات الاقتصادية الفلسطيني (ماس)، ملتزم بعمل أبحاث السياسات الاقتصادية والاجتماعية وفق أولويات التنمية في فلسطين بهدف المساعدة في صناعة السياسات الاقتصادية والاجتماعية وتعزيز المشاركة العامة في مناقشتها وصياغتها.

الأهداف الاستراتيجية

- ✧ عمل أبحاث ودراسات وفق أولويات واحتياجات صانعي القرار للمساعدة في اتخاذ قرارات ورسم سياسات مستندة للمعرفة.
- ✧ تقييم السياسات الاقتصادية والاجتماعية وتبيان تأثيرها على مختلف المستويات، وذلك لمراجعة وتصحيح السياسات المطبقة.
- ✧ توفير منبر حر للنقاش العام والديمقراطي حول قضايا السياسات الاقتصادية والاجتماعية للمهتمين وأصحاب الشأن.
- ✧ تقديم ونشر معلومات ونتائج الأبحاث الحديثة عن القضايا الاقتصادية والاجتماعية.
- ✧ تقديم الدعم الفني والمشورة المتخصصة لمؤسسات السلطة الوطنية الفلسطينية، والقطاع الخاص والمنظمات غير الحكومية لدعم مشاركتهم وانخراطهم في عملية صياغة السياسات.
- ✧ تقوية القدرات والمصادر لعمل أبحاث السياسات الاقتصادية والاجتماعية في فلسطين.

ص.ب. 19111، القدس وص.ب. 2426، رام الله

تلفون: 4/2987053، فاكس: 2987055، بريد إلكتروني: info@mas.ps

الصفحة الإلكترونية: www.mas.ps/

دراسة نقدية للأطر القانونية للجرائم الإلكترونية في الأراضي الفلسطينية

الباحث: محمد خليفة

المراجعة والتقييم: المحامي محمد ظرف

التمويل: تم إنجاز هذه الدراسة بدعم مشكور من قبل المصرف العربي للتنمية الاقتصادية في إفريقيا (BADEA) – البنك الأسلامي للتنمية (IDB) – صندوق الاقصى

معهد أبحاث السياسات الاقتصادية الفلسطيني (ماس)

القدس ورام الله

2012

تقديـــــم

مع توسع استخدامات الانترنت والهواتف الذكية في عرض ونقل المعلومات والوثائق وعمليات البيع والشراء وفي مختلف أعمال التعاقدات الأخرى، توسعت أيضاً أعمال سوء استخدام تلك الوسائل والي اشتمل على التخريب والاحتيال والغش والسرقة والخداع وغيرها من أشكال الجريمة التي بات يطلق عليها جرائم الكترونية.

وشكلت هذه التطورات السريعة والعاصفة في استخدامات التكنولوجيا الرقمية تحديات جديدة أمام أجهزة مكافحة الجريمة وتحقيق العدالة ونفاذ سيادة القانون. وحتم هذا على جميع الدول تطوير تشريعاتها وتطوير خبراتها وتجهيزاتها بصورة تمكنها من القيام بواجباتها تجاه المجتمع والأفراد وضمان استقراره. من هنا جاءت هذه الدراسة الاستكشافية التي طلبتها وزارة الاتصالات وتكنولوجيا المعلومات كمساهمة من المعهد لفتح نقاش جدي حول حجم المشكلات الناجمة عن استخدامات التكنولوجيا الرقمية والخيارات المتاحة أمام جهات صنع القرار في الاراضي الفلسطينية المحتلة لمواجهتها.

ومع نشر هذه الدراسة نود أن نشكر الباحثين وجميع من ساهم في تقديم المعلومات لفريق البحث ولمراجعي الدراسة والمشاركين في مناقشتها وتدقيق استنتاجاتها. ونخص بالذكر ممثلي وزارة الاتصالات وتكنولوجيا المعلومات والنيابة العامة ووزارة العدل في السلطة الوطنية الفلسطينية.

كما نتوجه بالشكر والتقدير للمصرف العربي للتنمية الاقتصادية في إفريقيا والبنك الإسلامي للتنمية–صندوق الأقصى على دعمهم لهذه الدراسة التي تعتبر واحدة من ضمن برنامج أبحاث أولويات السلطة الوطنية الفلسطينية.

د. سمير عبد الله
المديـــر العـــــام

شكر وامتنان

يود معهد أبحاث السياسات الاقتصادية الفلسطيني (ماس) أن يعبر عن امتنانه الشديد لمساهمة كوادر وموظفي المؤسسات المختلفة في إغناء هذه الدراسة، وفي تقديم اقتراحات بناءة في لتطويرها. ونخص بالشكر كل من السيدات والسادة: محمد العايدي مستشار وزير الاتصالات وتكنولوجيا المعلومات، وجمانة عبد ربه المساعد القانوني في وزارة الاتصالات وتكنولوجيا المعلومات، وطارق عسرواي وكيل نيابة مكافحة الجرائم الاقتصادية في النيابة العامة، والمحامي بلال كمال، ومصطفى فلنة مسؤول وحدة الجرائم الإلكترونية في القيادة العامة للشرطة، ونيفين أبو عيد رئيس قسم الدائرة القانونية في هيئة سوق رأس المال، وزيد الشوا القائم بأعمال مدير المكتب القانوني في سلطة النقد الفلسطينية، وحنان ياغي مسؤولة تكنولوجيا المعلومات في وزارة العدل، ولؤي الحسيني المستشار القانوني في وزارة العدل.

المحتويـــــــات

الملخص التنفيذي

تهدف هذه الدراسة إلى تحليل الأحكام المتعلقة بالجرائم الإلكترونية الواردة في كل من مشروع قانون المعاملات الإلكترونية ومشروع قانون العقوبات؛ لتحديد قدرة وكفاءة هذه البنود على مكافحة الجرائم الإلكترونية في فلسطين، وبالتالي تحليل أثرها على توفير بيئة أعمال مواتية لمختلف أشكال النشاط الاقتصادي. كما هدفت الدراسة إلى الإجابة على سؤال هام: هل الأراضي الفلسطينية بحاجة إلى قانون خاص بالجرائم الإلكترونية؟.

لتحقيق أهداف الدراسة تم اتباع مجموعة من الخطوات، أهمها: مراجعة الدراسات والتقارير التي تناولت الواقع التكنولوجي في الأراضي الفلسطينية، والاستفادة من تجارب عدد من الدول في مجال مكافحة الجرائم الإلكترونية، وعقد المقابلات الشخصية واللقاءات مع مختلف الأطراف ذات العلاقة، وذلك بهدف التعرف على آرائهم وتوجهاتهم إزاء مكافحة الجرائم الالكترونية. وعقد ورشة عمل متخصصة، دعي إليها الأطراف المعنية، وهدفت هذه الورشة التعرف على الآراء والتوجهات المتعددة لتلك الأطراف، وتوسيع دائرة المشاركة في النقاش والتحليل.

تجمع مختلف الأطراف ذات العلاقة بأن الجريمة الإلكترونية منتشرة في الأراضي الفلسطينية، وأن انتشارها بدأ بالتزايد منذ بضع سنوات. ولكن من الصعب إيجاد بيانات رسمية موثوقة حول عدد هذه الجرائم وأنواعها في الأراضي الفلسطينية بسبب عدم وجود قانون يحدد أنواع وعقوبات الجرائم الإلكترونية. ويعود انتشار الجرائم الإلكترونية إلى الأسباب التالية: زيادة عدد مستخدمي الإنترنت في الأراضي الفلسطينية؛ فقد بلغت نسبة الأسر التي لديها جهاز حاسوب 50.9% في العام 2011 وأن 30.4% من الأسر الفلسطينية لديها اتصال بالإنترنت في العام 2011 وترتفع نسبة المستخدمين من قبل الفئات الشبابية؛ فنحو 68.5% من الفئة العمرية 10–14 سنة يستخدمون الحاسوب، و81.4% من الفئة العمرية 15–19 سنة، و75.4% من الفئة العمرية 20–29 سنة. والسبب الآخر هو ارتفاع معدلات البطالة في الأراضي الفلسطينية؛ إذ بلغ معدل البطالة في الفترة 2001–2010 حوالي 25.3%، وتزداد خطورة البطالة على انتشار الجريمة الالكترونية بسبب انتشارها بين فئات الشباب. زد على ذلك عدم وجود القانون الذي يعالج الجريمة الإلكترونية ويعاقب على ارتكابها، وغيرها من الأسباب.

هناك وجهتا نظر فيما يتعلق بمدى الحاجة لسن قرار بقانون للجرائم الإلكترونية: ترى الأولى أن هناك ضرورة الإسراع في ذلك. وأن يتم إصداره بالاعتماد على نص المادة 43 من القانون الأساسي، أما وجهة النظر الأخرى فتعتقد أنه لا داع لإصدار قرار بقانون للجرائم الإلكترونية، حيث لا تنطبق حالة الضرورة على هذه الجرائم، ولا بد من انتظار انعقاد المجلس التشريعي، ويمكن عندئذ تقديم مشروع قانون للجرائم الإلكترونية ويسير في الإجراءات التشريعية العادية. من ناحية أخرى لا يتبين مدى الضرر الحاصل نتيجة للجرائم الإلكترونية، أو مدى تأثيرها السلبي على النواحي الاقتصادية أو الاجتماعية.

هناك وجهتا نظر فيما يتعلق بإصدار قانون مستقل للجرائم الإلكترونية: ترى وجهة النظر الأولى أن من الأفضل من الناحية القانونية إصدار قانون مستقل بالجرائم الإلكترونية، خاصة وأن قانون العقوبات يضع الإطار العام للعقوبات المختلفة ومن الصعب تعديله، كما أن مشروع قانون العقوبات قد يتأخر إصداره بسبب بعض المشكلات المتعلقة به. في حين أن تنظيم ما يتعلق بالجرائم الإلكترونية في قانون مستقل فيجعل تعديله أسهل بما يتناسب مع التطورات الإلكترونية المختلفة. في حين يرى بعض الخبراء القانونيين أنه وإن نصت بعض أحكام مشروع قانون

العقوبات على الجرائم الإلكترونية فإنه لا بد أيضاً من سن قانون مستقل للجرائم الإلكرتونية، من منطلق أن قانون العقوبات يشكل المظلة لكافة الجرائم. ولذلك، يجب أن تبقى الجرائم منصوص عليها في قانون العقوبات حتى لو صدر قانون للجرائم الإلكترونية أو قانون المعاملات الإلكترونية.

أهم النتائج التي توصلت إليها الدراسة هي:

- ✧ إن الجرائم الإلكترونية ظاهرة موجودة في الأراضي الفلسطينية، وأن انتشارها بدأ بالتزايد منذ بضع سنوات. إلا أنه لا يتوفر بيانات رسمية موثوقة حول مستويات انتشار وأنواع ومخاطر هذه الجرائم.
- ✧ يتأثر انتشار هذه الجرائم بانتشار استخدام الإنترنت في الأراضي الفلسطينية بشكل طردي، وبارتفاع معدلات البطالة، وعدم وجود القانون الملائم الذي يعاقب على الجريمة الإلكترونية، وغيرها من الأسباب.
- ✧ جاءت معظم النصوص المتعلقة بالجرائم الإلكترونية في مشروع قانون العقوبات الفلسطيني، وجاء جزء منها وهو المتعلق بتزوير التوقيع الإلكتروني وما شابه من الجرائم الإلكترونية في مشروع قانون المعاملات الإلكترونية. وهذا قد يسبب في تأجيل سن التشريع المتعلق بالجرائم الإلكترونية بسبب ما يتعلق بمشروع قانون العقوبات من بعض العوامل السياسية (تعطل عمل المجلس التشريعي... الخ) التي تؤجل إصداره.
- ✧ هناك كثير من أنواع الجرائم الإلكترونية التي وردت في كثير من قوانين الدول الأخرى لم تجر الإشارة إليها في كل من مشروع المعاملات الإلكترونية أو مشروع قانون العقوبات مثل المقامرة، والاتجار بالأسلحة والذخائر، والاتجار بالتحف الفنية.
- ✧ إن عقوبة الحبس التي وردت ضمن العقوبات المفروضة على الجرائم الإلكترونية دون أن تحديد مدته يعد خللاً في مشروع القانون. فقد ورد فرض هذه العقوبة 10 مرات دون تحديد مدة الحبس، مما يضعف من وظيفة القانون لردع الجريمة الالكترونية، ويخلق غموضا لا مبرر له ويجعل من تحقيق العدالة أمرا صعبا.
- ✧ لا تتناسب العقوبات أحياناً مع الأثر المترتب على الجريمة الإلكترونية.
- ✧ لم يرد في النصوص المتلعقة بالجرائم الإلكترونية بعض الإجراءات الأخرى للحد من الجرائم الإلكترونية، مثل إنشاء محكمة خاصة للجرائم الإلكترونية، وإنشاء نيابة متخصصة في جرائم المعلوماتية، إنشاء شرطة متخصصة لجرائم المعلوماتية.

على ضوء النتائج التي توصلت إليها الدراسة، فإنها تقترح التوصيات التالية:

- ✧ العمل على صياغة مشروع قانون خاص بالجرائم الإلكترونية أسوة بمعظم الدول الأخرى.
- ✧ أن ينص على أنواع أخرى من الجرائم الإلكترونية التي لم ترد في أي من مشروعي قانوني العقوبات والمعاملات الإلكترونية، وأهمها استخدام الشبكة المعلوماتية أو تقنية المعلومات للقيام بأي مما يلي: استخدام تقنية المعلومات في المقامرة أو الترويج لبرامج أو أفكار أو أنشطة من شأنها ذلك، والاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية السلامة العامة أو الاقتصاد الوطني، والدخول بغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات خاصة بالمنشآت المالية والتجارية والاقتصادية، وإنشاء موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار بالأسلحة والذخائر أو تسهيل التعامل فيها. وأن يشمل القانون على الشروط والضمانات التي توفر الحماية

الكافية لحقوق الإنسان والحريات الأساسية الأخرى، وأن لا يتعارض تطبيق أحكام القانون الأحكام المتعلقة بحرية الصحافة وحرية التعبير.

- ✧ هناك بعض الأمور الهامة التي يجب مراعاتها فيما يتعلق بالعقوبات: أن يعمل مشروع القانون بتحديد المدة الزمنية لعقوبة السجن أو أن يضع حداً أدنى وحداً أعلى لمدة الحبس، وأن يضع حداً أدنى وحداً أعلى لقيمة الغرامة المالية كذلك، وأن يراعي المشروع ملائمة العقوبة للجريمة بحيث تكون العقوبة أشد كلما كانت الجريمة أكبر أو أثرها سلبياً أكثر، وغيرها.
- ✧ أن يشير المشروع إلى بعض القضايا الهامة الأخرى مثل: أن تأخذ قضايا الجرائم الإلكترونية صفة الاستعجال، وانتداب قاض متخصص للبت في الجرائم الإلكترونية، وضرورة التعاون بين الدول والقطاع الخاص في مكافحة الجرائم الإلكترونية، والتعاون الدولي لمكافحة الجريمة الحاسوبية.
- ✧ إضافة إلى سن قانون للجرائم الإلكترونية هناك ضرورة للقيام بالتوعية بخطورتها وتأثيرها على المجتمع باستخدام مختلف الوسائل، ومنها على سبيل المثال: لإشارة إلى هذه الجرائم في المناهج المدرسية وفي مساقات الجامعات، وإصدار نشرات توعية للتعريف بها وبخطورتها، وعقد ورش عمل مختلفة ولفئات مختلفة من المجتمع تتناول الحديث عن هذه الجرائم، وتصميم برامج في الإذاعة والتلفزيون تتناول ما يتعلق بهذه الجرائم، ونشر بعض القصص بالرموز أو بأسماء وأماكن وهمية.
- ✧ الاستعانة ببرامج أمن قوية ضد الفيروسات أو اختراقات أنظمة الحاسوب.
- ✧ نظراً لتمتع مرتكبي الجرائم الإلكترونية بقدرات خاصة ومميزة فإنه يمكن الاستفادة من خبراتهم في تعزيز الحماية الإلكترونية للمؤسسات المختلفة.
- ✧ العمل على عقد دورات تدريبية في كافة الجوانب المتعلقة بالجرائم الإلكترونية للعاملين في الجهات ذات العلاقة مثل أفراد الشرطة، والنيابة العامة والقضاة.

1- الجرائم الإلكترونية في الأراضي الفلسطينية

المقدمة

يعد التطور الكبير في تكنولوجيا الإعلام والاتصال وظهور الشبكة العالمية "الإنترنت" أحد مميزات العصر الحالي، وقد كان له كثير من الآثار الإيجابية في الجوانب المختلفة، حيث ساهم بشكل عام في تطور وتغيير نمط حياة الأفراد والمجتمعات. ولكن في المقابل كان لهذا التطور التكنولوجي العظيم العديد من الآثار الجانبية السلبية على حياة الناس والشركات والمؤسسات والدول أيضا. وقد تمثل ذلك في استغلال الإنترنت والوسائل الالكترونية لممارسة الجريمة. وهكذا ظهرت إلى الوجود الجرائم الالكترونية، التي يراها الخبراء على أنها الابن غير الشرعي للتكنولوجيا، والتي انتشرت بشكل واسع بحكم التزامن بين ثورة تكنولوجيا المعلومات والعولمة.

وللجريمة الإلكترونية عدة مسميات: منها جرائم الحاسوب والإنترنت (Computer Crime)، وجرائم التقنية العالية (Hi-Tech Crime)، والجريمة الإلكترونية (E-Crime)، والجريمة السيبرانية (Cyber Crime) ، وجرائم أصحاب الياقات البيضاء (White Collar) . وهناك أكثر من تعريف للجريمة الإلكترونية يعتمد على المعيار المستخدم في التعريف، وتتمحور هذه التعريفات حول الارتكاب المتعمد لفعل ضار من الناحية الاجتماعية أو فعل خطير محظور يعاقب عليه القانون. وأفضل هذه التعريفات تعريف خبراء متخصصون من بلجيكا بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأمواج المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية". ويعرفها خبراء منظمة التعاون الاقتصادي والتنمية، بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها" (عرب، 2006).

كانت أول جريمة إلكترونية موثقة في العام 1959 مع بدء ظهور الإنترنت الذي كان متاحاً في البداية لمراكز الأبحاث والجامعات، ثم تطور الإنترنت ليصبح شبكة اتصالات دولية، وفي أواسط التسعينيات أصبح الإنترنت متاحاً لجمهور كبير من الناس، وبدأت الجرائم الإلكترونية بالانتشار. وأشارت دراسة مسحية أجرتها شركة نورتن العالمية المتخصصة في تطوير الحلول البرمجية الأمنية في العام 2010، أن نحو ثلثي مستخدمي الإنترنت (65٪) وقعوا ضحية للجريمة الإلكترونية مرة واحدة على أقل تقدير، وتمثّل ذلك في الهجمات الفيروسية أو التجسسية أو الاحتيالية لسرقة بيانات البطاقات الائتمانية أو سرقة الهوية والبيانات المصرفية والشخصية لاستغلالها في أغراض إجرامية (www.emaratalyoum.com).

وتنصب هذه الجرائم على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتعتدي على حق ملكية المعلومات، ويستخدم لارتكاب هذه الجرائم وسائل تقنية تقتضي استخدام الحاسوب بوصفه أداةً حققت التزاوج بين تقنيات الحوسبة والاتصالات. إضافة إلى الحاسوب بدأ حديثاً استخدام أجهزة الاتصال الخلوية والتي يوجد بها العديد من القدرات التي لا تقل في بعضها عما تقوم به أجهزة الحاسوب.

وتتسم الجرائم الإلكترونية بالخطورة العالية نظرا لأغراضها المتعددة قياسا بالجرائم التقليدية. وهناك عدة مشكلات ومعيقات إدارية وقانونية في تحقيق وتحري هذه الجرائم وتطبيق العقوبات عليها. ويزداد الأمر تعقيداً عند الحديث

عن الجرائم الالكترونية كونها عابرة للحدود السياسية والجغرافية بفعل ارتباط العالم بشبكة واحدة والانتشار الواسع للمعلومات. وتثير مسألة التباعد الجغرافي كثيراً من المشكلات في مجال هذه الجرائم وبشكل خاص الإجراءات الجنائية وجهات الاختصاص والقانون الواجب التطبيق.

كما أن لهذه الجرائم العديد من الآثار السلبية على جوانب الحياة المختلفة سواء السياسية أو الاجتماعية أو الثقافية أو الاقتصادية. وقد تنجم عن هذه الجرائم خسائر فادحة، خاصة ما يتعلق بسرقة البطاقات الإئتمانية أو غسيل الأموال، أو الاحتيال وغيرها. من هنا عملت كثير من الدول على سن قانون للجرائم الإلكترونية لمكافحة هذه الظاهرة، وأصبح هذا القانون جزء من منظومة توفير سيادة القانون وتحقيق العدالة، وحماية حقوق الأفراد والجماعات والمؤسسات.

ولمواجهة الجرائم الإلكترونية قامت كثير من الدول بعقد العديد من المؤتمرات التي تتناول جوانب مختلفة تتعلق بهذه الجرائم، إضافة إلى تأسيس وحدات أو دوائر خاصة بالجرائم الإلكترونية في الإدارات العامة للشرطة، وكذلك سن قوانين خاصة بهذه الجرائم، وتعد السويد الدولة الأولى التي وضعت تشريعاً يتناول الجرائم الإلكترونية في العام 1973، ثم تبعها العديد من الدول الأخرى. وبدأت الدول العربية منذ العام 2004 بسن قوانين للجرائم الإلكترونية مثل الإمارات والأردن وعمان وسوريا. أما فيما يتعلق بالجهد الفلسطيني في هذا المجال، فقد تم إعداد مشروع قانون المعاملات الإلكترونية في حزيران 2011، الذي اشتمل على بعض العقوبات المتعلقة بالجرائم الإلكترونية في مجال التوقيعات الإلكترونية، إضافة إلى وضع فصل خاص في مشروع قانون العقوبات لسنة 2010 تناول عقوبات لمجموعة أخرى من الجرائم الإلكترونية. وجدير بالذكر أن مكافحة هذه الجرائم تتطلب تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد أنواعها وقواعد التسليم فيها وإيجاد الحلول لمشكلاتها الأساسية.

هدف الدراسة:

تهدف هذه الدراسة إلى تحليل البنود المتعلقة بالجرائم الإلكترونية الواردة في كل من مشروع قانون المعاملات الإلكترونية ومشروع قانون العقوبات؛ لتحديد قدرة وكفاءة هذه البنود على مكافحة الجرائم الإلكترونية في فلسطين، وبالتالي تحليل أثرها على توفير بيئة أعمال مواتية لمختلف أشكال النشاط الاقتصادي. ستقوم الدراسة بتحديد نقاط القوة والضعف في هذه الأحكام؛ بغية الوصول إلى توصيات محددة حول التعديلات المطلوبة من أجل الوصول إلى اطار قانوني شامل وفعال لمكافحة الجرائم إلكترونية وبما يسهم في الحد من انتشارها في فلسطين. ستركز الدراسة على تحليل الأبعاد الاقتصادية والاجتماعية للأحكام والمواد الواردة في القانونين المذكورين، بينما تترك الصياغات القانونية للمختصين في هذا المجال.

إضافة إلى هذا الهدف الرئيس للدراسة، فإنها تسعى إلى تحقيق أهداف فرعية أخرى:

- ✧ الإجابة على سؤال هام: هل الأراضي الفلسطينية بحاجة إلى قانون خاص بالجرائم الإلكترونية؟
- ✧ التعريف بالجرائم الإلكترونية، وخصائصها، وسرد بعض الأمثلة عليها. ومدى انتشارها في الأراضي الفلسطينية المحتلة. والإجراءات التي اتخذتها السلطة الفلسطينية والمؤسسات الأخرى للحد من هذه الجرائم.

- ✧ مقارنة الأحكام الخاصة بالجرائم الإلكترونية مع القوانين الأخرى سارية المفعول في الضفة الغربية وقطاع غزة؛ لمعرفة مدى انسجامها مع منظومة القوانين؛ بهدف إزالة التعارض أو عدم الانسجام مع هذه القوانين إن وجد. مع الأخذ بالاعتبار التطورات الحديثة على الساحتين الإقليمية والدولية، وبخاصة العولمة، وثورة المعلومات، والتجارة الإلكترونية، والانفتاح العالمي، وغيرها.
- ✧ مقارنة أحكام الجرائم الالكترونية الواردة في مشروعي قانوني المعاملات الإلكترونية والعقوبات مع القوانين الشبيهة في دول أخرى وخاصة في بعض الدول المجاورة، ذات النظام القضائي الشبيه بالنظام القضائي الفلسطيني، وذات النظام الاقتصادي الشبيه بالاقتصاد الفلسطيني ، إضافة إلى مقارنتها مع القوانين في بعض الدول المتقدمة مثل السويد واليابان وبريطانيا وفرنسا، وذلك للاستفادة من تجارب هذه الدول في تحسين صياغة مشروع القانون.

أهمية الدراسة

تنبع أهمية هذه الدراسة من تناولها موضوعاً جديداً وعصريا، وهو الجرائم الإلكترونية، التي قد تمس حقوق كل شخص يستخدم التكنولوجيا الحديثة سواء الحاسوب أو الهاتف الخلوي أو بطاقة الصراف الآلي وغيرها. وتحاول هذا الدراسة اكتشاف مدى انتشار هذه الجرائم في الأراضي الفلسطينية. ويتوقع أن تسهم هذه الدراسة في اقتراح بعض التعديلات الضرورية على عدد من المواد والأحكام الواردة في مشروعي قانوني المعاملات الإلكترونية والعقوبات التي اشتملت على مواد لمكافحة هذه الجرائم، بحيث تؤدي تلك التعديلات إلى تطوير الأحكام القانونية ذات العلاقة، وتحقيق شمولها وزيادة قدرتها على التجاوب والتعامل مع التطورات التكنولوجية في مجالات المعلوماتية والاتصالات، وبالتالي الحد من انتشار الجرائم الإلكترونية. ومن ثم تحقيق الاستخدام الآمن لتكنولوجيا المعلومات في كافة أنواع النشاطات الاقتصادية والإنسانية.

منهجية الدراسة

لتحقيق أهداف الدراسة سيتم اتباع مجموعة من الخطوات، أهمها:

- ✧ مراجعة الدراسات والتقارير التي تناولت الواقع التكنولوجي في الأراضي الفلسطينية، وذلك من أجل التعرف على المشكلات أو الجرائم الناجمة عن استخدام التكنولوجيا، ومدى انتشارها.
- ✧ الاستفادة من تجارب عدد من الدول في مجال مكافحة الجرائم الإلكترونية، إذ تمثل تجارب الدول الأخرى محاولة لاختيار التطبيق الأمثل للاستفادة من هذه التجارب في صياغة مشروع القانون، أو اقتراح السياسات الملائمة مع الأخذ بالاعتبار خصوصية الحالة الفلسطينية.
- ✧ عقد المقابلات الشخصية واللقاءات مع مختلف الأطراف ذات العلاقة، وذلك بهدف التعرف على آرائهم وتوجهاتهم إزاء مكافحة الجرائم الالكترونية. وتشمل هذه المقابلات بشكل رئيس المسؤولين في الوزارات والجهات الرسمية ذات العلاقة، وممثلين عن الشركات العاملة في هذا المجال، وخبراء فنيين وقانونيين.
- ✧ عقد ورشة عمل متخصصة، يدعي إليها الأطراف المعنية، وهدف هذه الورشة التعرف على الآراء والتوجهات المتعددة لتلك الأطراف، وتوسيع دائرة المشاركة في النقاش والتحليل.

محتوى الدراسة

تتكون الدراسة من خمسة أجزاء:

الجزء الأول: ويتكون من المقدمة التي تظهر الأهداف التي تسعى الدراسة إلى تحقيقها، وأهمية الدراسة، والمنهجية المتبعة في إعدادها.

الجزء الثاني: يبحث في واقع الجرائم الإلكترونية في الأراضي الفلسطينية، ومدى الحاجة إلى قانون للجرائم الإلكترونية.

الجزء الثالث: يعطي لمحة عن خصائص الجرائم الإلكترونية، وبعض الأمثلة عليها في بعض الدول.

الجزء الرابع: يتناول مقارنة أحكام المواد المتعلقة بمكافحة الجرائم الالكترونية في مشروعي قانوني المعاملات الإلكترونية والعقوبات مع القوانين الأخرى سارية المفعول في الضفة الغربية وقطاع غزة، لمعرفة مدى انسجامها مع منظومة القوانين؛ بهدف إزالة التعارض أو عدم الانسجام مع هذه القوانين إن وجد.

الجزء الخامس: يتناول تجارب عدد من الدول مقارنة بالتجربة الفلسطينية في مجال سن قوانين للجرائم الإلكترونية.

الجزء السادس: يستعرض أهم النتائج التي توصلت إليها الدراسة، والتوصيات التي يمكن أن تسهم في تطوير الإطار القانوني الذي يعمل على مكافحة الجرائم الإلكترونية والحد منها.

2- واقع الجرائم الإلكترونية في الأراضي الفلسطينية ومدى الحاجة إلى قانون خاص بها

يسلط هذا الجزء الضوء على واقع الجرائم الإلكترونية في الأراضي الفلسطينية، ومدى انتشارها. ويناقش مدى الحاجة إلى سن قانون خاص بالجرائم الإلكترونية.

2-1 مدى انتشار الجرائم الإلكترونية في الأراضي الفلسطينية

تجمع مختلف الأطراف ذات العلاقة بأن الجريمة الإلكترونية منتشرة في الأراضي الفلسطينية، وأن انتشارها بدأ بالتزايد منذ بضع سنوات. وبسبب عدم وجود قانون يحدد أنواع وعقوبات الجرائم الإلكترونية، فمن الصعب إيجاد بيانات رسمية موثوقة حول عدد هذه الجرائم وأنواعها في الأراضي الفلسطينية؛ فقد تبين للباحث من خلال الاتصال مع مجلس القضاء الأعلى أنه لا يوجد في المحاكم الفلسطينية قضايا جرائم إلكترونية. ويرجع ذلك إلى أن هذه الجرائم يتم تصنيفها تحت بند الجرائم الأخرى التي يوجد نصوص قانونية تجرمها وتضع هقوبة لها؛ فعلى سبيل المثال فإن جرائم التشهير على الإنترنت تصنف تحت بند جرائم القدح والذم. ومن الصعوبة بمكان معرفة عدد الجرائم الإلكترونية أو إعادة تصنيفها بدون وجود القانون الذي يحدد ماهيتها وأنواعها والعقوبات المتعلقة بها. حيث أنه وبموجب المادة 15 من القانون الأساسي المعدل التي نصت على أن:" العقوبة شخصية، وتمنع العقوبات الجماعية، ولا جريمة ولا عقوبة إلا بنص قانوني، ولا توقع عقوبة إلا بحكم قضائي، ولا عقاب إلا على الأفعال اللاحقة لنفاذ القانون".

ويعود انتشار الجرائم الإلكترونية إلى الأسباب التالية:

- زيادة عدد مستخدمي الإنترنت في الأراضي الفلسطينية

أدى انتشار خدمات الإنترنت وانخفاض تكلفة الاشتراكات، إلى زيادة عدد مستخدمي الإنترنت، كما جعلت الإنترنت أكثر شعبية، ووسيلة مريحة للاتصال، كما أنها فتحت أبوابًا جديدة للأعمال على الإنترنت، فقد بلغت نسبة الأسر التي لديها جهاز حاسوب 50.9% في العام 2011 مقارنة مع 26.4% في العام 2004، بواقع 53.2% في الضفة الغربية و46.5% في قطاع غزة. وأشار 49.4% من الأسر التي ليس لديها حاسوب أن السبب الرئيس وراء عدم اقتنائها الحاسوب هو ارتفاع أسعار أجهزة الحاسوب، في حين أشار 23.2% أن السبب وراء ذلك هو عدم وجود شخص مؤهل لاستخدام الحاسوب (الجهاز المركزي للإحصاء الفلسطيني، 2011).

وأن 30.4% من الأسر الفلسطينية لديها اتصال بالإنترنت في العام 2011 مقارنة مع 9.2% في العام 2004، وتتقارب مستويات الاستخدام بين الضفة الغربية وقطاع غزة، وأن 39.6 من الأفراد الذين يستخدمون الحاسوب ممن بلغو عمر 10 سنوات فأكثر في العام 2011 مقارنة مع 32.3% في العام 2009. كما ترتفع نسبة المستخدمين من قبل الفئات الشبابية؛ فنحو 68.5% من الفئة العمرية 10-14 سنة يستخدمون الحاسوب، و81.4% من الفئة العمرية 15-19 سنة، و75.4% من الفئة العمرية 20-29 سنة. ثم تأخذ النسبة بالانخفاض مع زيادة العمر إذ بلغت النسبة 37% للفئة العمرية 50 سنة فأكثر. كما أن 69.7% من الأفراد 10 سنوات فأكثر يمتلكون بريد إلكتروني (الجهاز المركزي للإحصاء الفلسطيني، 2011).

أما الغرض الرئيس من استخدام الإنترنت يأتي بالدرجة الأولى الاتصال بنسبة 22.6%، ثم التسلية والترفيه بنسبة 19%، والدراسة 16.1%، والاطلاع والمعرفة 11.3%، والعمل 9.6%، والمواضيع العلمية 6.5%، والمواضيع السياسية والأخبار 6%، ثم المواضيع الأخرى. من ناحية أخرى فإن عدد أجهزة الحاسوب المتوفرة لدى الأسر لا يعكس بشكل تام مدى استخدام الإنترنت، حيث تنتشر هذه الخدمة في المقاهي العامة، والنوادي، وعلى أجهزة الهاتف النقال وغيرها. وبالتالي، من المتوقع أن تؤدي زيادة استخدام الإنترنت ارتفاع نسبة إساءة الاستخدام أيضًا. ويفاقم من هذه الظاهرة عدم وجود برامج توعية، مما يعرض أعدادا متزايدة من مُسْتَخْدمي الإنترنت للاختراقات والجريمة الإلكترونيَّة.

- ارتفاع معدلات البطالة في الأراضي الفلسطينية؛ تعد البطالة إحدى المشكلات الرئيسة والمزمنة التي تواجه الاقتصاد الفلسطيني؛ إذ بلغ معدل البطالة في الفترة 2001–2010 حوالي 25.3%، وقد بلغ عدد العاطلين عن العمل 231 ألف شخص في العام 2010 شكلوا 23.7% من القوى العاملة، بواقع 17.2% في الضفة الغربية، و37.8% في قطاع غزة. (الجهاز المركزي للإحصاء الفلسطيني، 2011).

وتزداد خطورة البطالة على انتشار الجريمة الالكترونية بسبب انتشارها بين فئات الشباب؛ إذ بلغت نسبة البطالة في الفئة العمرية 15–24 عاماً 28.2% وللفئة العمرية 25–34 عاماً 18.2%، بمعنى ان نسبة كبيرة من العاطلين عن العمل هم من خريجي الجامعات، الذين غالباً يكون لديهم معرفة باستخدام الحاسوب والإنترنت؛ مما يؤدي إلى زيادة انتشار الجريمة الإلكترونية.

- عدم وجود القانون الذي ينظم ويعاقب على الجريمة الإلكترونية يساعد على انتشار هذه الجرائم، فكما اتضح من خلال المقابلات الشخصية مع الجهات المختلفة فإن كثيراً من الأفعال التي تعتبر مخالفة قانونية لا يتم معاقبة مرتكبها في حالة ارتكابها إلكترونيا لعدم وجود النص القانوني[1].
- القصور في برامج التوعية الأمنية: إن نشر برامج التوعية بأمن المعلومات من أكثر الطرق فعالية في محاربة الجريمة الإلكترونية، فهناك نقص شديد في برامج التوعية بأمن المعلومات على مستوى الأفراد والمؤسسات والحكومات. وقد يستغل المجرمون عوامل قلة فعالية برامج التّوعية بأَمْنِ المعلومات المتاحة في ارتكاب مثل هذه الجرائم.
- عدم وجود سيادة فلسطينية على المجال الكهرممغناطيسي، والتشابك مع شبكات الانترنت والاتصالات الإسرائيلية يعقد من إمكانات متابعة الجرائم الإلكترونية، كما لا يسمح للسلطات الفلسطينية المختصة بحجب بعض المواقع التي تشكل مصدرا للجريمة القانونية بالمفهوم الفلسطيني.

2-2 أنواع الجرائم الإلكترونية المنتشرة في الأراضي الفلسطينية

أما فيما يتعلق بأنواع الجرائم الإلكترونية المنتشرة في الأراضي الفلسطينية، فقد تبين للباحث من خلال لقاء الجهات المختلفة أنها تتركز في الأنواع التالية:

- الدخول إلى المواقع الإلكترونية الرئيسة لشركة جوال أو الاتصالات أو شركة حضارة، وتسديد فواتير للمتسللين.

[1] على سبيل المثال، قام شاب ومن خلال محادثة عبر الإنترنت بتصوير فتاة بأوضاع مخلة، وتم نشرها على موقع الفيس بوك الإلكتروني، ولكن بعد وصول القضية إلى المحكمة، لم يجد القاضي نصاً قانونياً يجرم هذا السلوك، وتم تبرئة الشاب بحجة أن ما تم كان برضا الفتاة (مقابلة مع وحدة الجرائم الإلكترونية في الشرطة).

- سرقة كلمة المرور للبريد الإلكتروني، وإرسال رسائل مختلفة منه، مثال ذلك ما حدث في محافظة الخليل؛ حيث تعددت أعمال بعض "الهكرز"، وهم المتمترسون على صفحات الويب والذين بإمكانهم سرقة البرامج المختلفة، إلى اللجوء مؤخرا للابتزاز والنصب من خلال استخدام بعض الإيميلات وصفحات الفيس بوك للحصول على الأموال، وخاصة بمحافظة الخليل. وتقوم طريقة المبتزين بسرقة حساب شخصي لأحد الأشخاص وطلب المال أو أرصدة جوال بطريقة الاستعطاف، ويعطي الشخص الذي تتم المحادثة معه رقم هاتف يدعي أنه لأمه (الشخص المبتز)، وبالفعل اتصل بعض الضحايا بهذا الرقم وتم استعطافهم من قبل إمرأة عجوز بحاجة إلى مبلغ من المال، أو رصيد جوال بطريقة التسول. وحول العديد من الضحايا أرصدة لهؤلاء المبتزين، ولم تقتصر أهداف الهكرز على التسول والابتزاز بل تعدى ذلك بأنهم قاموا بتخريب علاقات اجتماعية بين الضحايا، والتشهير بهم، فكل ضحية اعتقدت أن صديقها قام بسرقة الإيميل أو الحساب الشخصي لها على الفيس بوك ما أدى إلى اتخاذ بعضهم إجراءات عدة كالاتصال بالشرطة وغيرها كادت ان توقع الفتنة بين صفوف المواطنين في مدينة الخليل. وقد وصلت عدة شكاوى إلى الجهات الأمنية في محافظة الخليل وعند البحث والتحري تبين أن العصابة من قطاع غزة. وهي تعمل في النصب والاحتيال عن طريق شبكة الإنترنت ويستهدفون الأفراد في الضفة الغربية حتى لا يتعرضوا للملاحقة والمساءلة (جريدة القدس، 2011).

من ناحية أخرى أفادت وزارة الاتصالات وتكنولوجيا المعلومات أن الأراضي الفلسطينية المحتلة مصنفة على القائمة السوداء فيما يتعلق بإرسال الرسائل عبر البريد الإلكتروني، حيث تصل هذه الرسائل إلى الدول الأخرى على أنها رسائل غير مرغوب فيها (Spam).

- الجرائم الجنسية مثل تصوير فتيات في أوضاع مخلة من خلال المحادثة الإلكترونية، ثم ابتزازهن للحصول على الأموال أو تنفيذ سلوك معين.
- الحصول على معلومات يمنع الوصول إليها، كما حدث في تسريب دليل المشتركين في شركة جوال.
- اختراق بعض المواقع الإلكترونية، كما حدث مثلاً أن قام شاب من قطاع غزة باختراق الحاسوب الرئيس لدولة البرتغال.
- سرقة العديد من بطاقات الصراف الآلي، ومحاولة سرقة الأموال من خلالها.
- التشهير والقدح والذم وخاصة من خلال مواقع التواصل الاجتماعي مثل موقع الفيس بوك.
- التغرير ومحاولة الاحتيال من خلال إرسال رسائل إلكترونية للشخص بأنه ربح مبلغ معين ويطلب منه معلومات وبيانات مالية ورقم حسابه في البنك وتحويل أموال للجهة التي أرسلت الرسالة.

2-3 مدى الحاجة لسن قانون للجرائم الإلكترونية

كما ذكر سابقاً لا يتوفر بيانات حول عدد الجرائم الإلكترونية ومجالات انتشارها، مما يجعل من الصعوبة بمكان دراسة تأثير الجرائم الإلكترونية على النواحي المختلفة وخاصة الاقتصادية منها. وتبين للباحث نتيجة للمقابلات الشخصية مع الأطراف المختلفة أن هناك خلاف على أمرين:

- مدى الحاجة لسن قرار بقانون للجرائم الإلكترونية، أي إصداره من قبل الرئيس في ظل غياب المجلس التشريعي.

- ✧ أفضلية إصدار قانون مستقل للجرائم الإلكترونية، أو الإبقاء على نصوص قانونية في مشروعي قانوني المعاملات الإلكترونية والعقوبات.

ففيما يتعلق بالأمر الأول وهو مدى الحاجة لسن قرار بقانون للجرائم الإلكترونية هناك وجهتا نظر:

- ✧ ترى بعض الجهات مثل وزارة الاتصالات وتكنولوجيا المعلومات أنه من الضرورة الإسراع في سن قرار بقانون للجرائم الإلكترونية تحت اسم قرار بقانون بشأن الجرائم الإلكترونية؛ نتيجة للانتشار الكبير لهذه الجرائم. مما حدا بالسلطة الفلسطينية إلى اتخاذ العديد من الإجراءات للحد منها والعمل على مكافحتها، وأهم هذه الإجراءات:

- إنشاء وحدة مكافحة الجرائم الإلكترونية في القيادة العامة للشرطة الفلسطينية وذلك منذ بداية العام 2011، حيث تهدف هذه الوحدة إلى التحقيق في الجرائم الإلكترونية، وتقديم المتهمين بالقيام بها إلى القضاء.
- إفراد فصل خاص لجرائم تقنية المعلومات في مشروع قانون العقوبات الفلسطيني.
- تحديد العقوبات المتعلقة بكل جريمة إلكترونية فيما يتعلق بالمعاملات الإلكترونية في مشروع قانون المعاملات الإلكترونية.

وترى هذه الجهات أن هناك العديد من المبررات التي تتطلب سن هذا القرار بقانون، والتي أهمها وجود العديد من قضايا الجرائم الإلكترونية العالقة في المحاكم الفلسطينية، وعدم القدرة على البت فيها لعدم وجود النص القانوني. إضافة إلى تضرر شريحة كبيرة من المجتمع جراء هذه الجرائم، مما يتطلب وجود نص قانوني يجرم هذه الأفعال ويوقع العقوبة الملائمة عليها، وعدم وجود هذا القانون يؤدي إلى ضياع حقوق كثير من المواطنين. إضافة إلى أن هناك ضرر اقتصادي يلحق بالعديد من الشركات بسبب تعرضها للاحتيال، حيث أن قانون العقوبات رقم 19 لسنة 1960 المطبق حالياً هو قانون قديم ولا ينص على تجريم الأفعال الإلكترونية المختلفة التي تلحق ضرراً بالغاً بالآخرين، ويؤدي استمرار غياب هذا القانون إلى انتشار المزيد من الجرائم الإلكترونية.

ونتيجة لهذه المبررات هناك ضرورة للإسراع في تطوير وتحديث القوانين ذات العلاقة أو سن قرار بقانون خاص وشامل لمكافحة الجرائم الالكترونية وعدم انتظار انعقاد المجلس التشريعي الفلسطيني، وأن يتم إصداره بالاعتماد على نص المادة 43 من القانون الأساسي المعدل لسنة 2003 والتي نصت على:" لرئيس السلطة الوطنية في حالات الضرورة التي لا تحتمل التأخير في غير أدوار انعقاد المجلس التشريعي، إصدار قرارات لها قوة القانون، ويجب عرضها على المجلس التشريعي في أول جلسة يعقدها بعد صدور هذه القرارات وإلا زال ما كان لها من قوة القانون، أما إذا عرضت على المجلس التشريعي على النحو السابق ولم يقرها زال ما يكون لها من قوة القانون".

- ✧ يرى بعض الخبراء في مجال القانون أنه لا تنطبق حالة الضرورة لإصدار قرار بقانون للجرائم الإلكترونية، من ناحيتين: أنه تفسير المادة 43 من القانون الأساسي فإن سن هذا القانون ليس بهذه الضرورة لكي يصدر قراراً بقانون، ولا بد من انتظار انعقاد المجلس التشريعي، ويمكن عندئذ تقديم مشروع قانون للجرائم الإلكترونية ويسير في الإجراءات التشريعية العادية. من ناحية أخرى لا يتبين مدى الضرر الحاصل نتيجة للجرائم الإلكترونية، أو مدى تأثيرها السلبي على النواحي الاقتصادية أو الاجتماعية. وبالتالي، ليس هناك داع

للعجلة في إصدار قرار بقانون للجرائم الإلكترونية؛ خاصة وأن سن أي قانون من المفروض أن يعكس الواقع الثقافي والاجتماعي والسياسي في المجتمع.

أما فيما يتعلق بأفضلية إصدار قانون مستقل للجرائم الإلكترونية، أو الإبقاء على نصوص قانونية في مشروعي قانوني المعاملات الإلكترونية والعقوبات. أيضاً هناك وجهتا نظرحول هذا الأمر:

- يرى معدو مشروع قانون المعاملات الإلكترونية وبعض الخبراء في المجال الإلكتروني أن من الأفضل من الناحية القانونية إصدار قانون مستقل بالجرائم الإلكترونية يوضع به كافة القضايا المتعلقة بالجرائم الإلكترونية، وأن هناك حاجة أكبر لسن رزمة من القوانين ذات الشأن الإلكتروني، خاصة وأن قانون العقوبات يضع الإطار العام للعقوبات المختلفة ومن الصعب تعديله، كما أن مشروع قانون العقوبات قد يتأخر إصداره بسبب بعض المشكلات المتعلقة به[2]. في حين أن تنظيم ما يتعلق بالجرائم الإلكترونية في قانون مستقل فيجعل تعديله أسهل بما يتناسب مع التطورات الإلكترونية المختلفة. كما أن معظم الدول الأخرى وضعت قانوناً خاصاً بالجرائم الإلكترونية كما سيأتي ذكره في الجزء الخامس.
- يرى بعض الخبراء القانونيين أنه وإن نصت بعض أحكام مشروع قانون العقوبات على الجرائم الإلكترونية فإنه لا بد أيضاً من سن قانون مستقل للجرائم الإلكرتونية، من منطلق أن قانون العقوبات يشكل المظلة لكافة الجرائم. ولذلك، يجب أن تبقى الجرائم منصوص عليها في قانون العقوبات حتى لو صدر قانون للجرائم الإلكترونية أو قانون المعاملات الإلكترونية.

ولكن من الناحية العملية فإن من المهم أن يكون هناك نص قانوني يجرم الأفعال الإلكترونية المختلفة بالاعتداء على الآخرين، وليس المهم أن يكون ذلك في قانون مستقل أو وجدت نصوص في قانونين.

من ناحية أخرى فإن سن قانون يعاقب على ارتكاب الجرائم الإلكترونية هو أمر ضروري، ولكن القانون يعاقب على الجريمة بعد ارتكابها ويحاسب من يقترفها. ولكن هناك ضرورة ملحة أخرى تتمثل في محاولة الحد من حدوث هذه الجرائم. فكما أشرنا سابقا أن هذه الجرائم تتميز بخصائص معينة يصعب معها إثباتها أو التحقيق فيها أو اكتشاف هوية مرتكبها. لذا لا بد أن يصار إلى تكثيف جهود التوعية بخطورتها وتأثيرها على المجتمع باستخدام مختلف الوسائل، ومنها على سبيل المثال:

- يمكن الإشارة إليها في المناهج المدرسية وفي مساقات الجامعات.
- إصدار نشرات توعية للتعريف بها وبخطورتها.
- عقد ورش عمل مختلفة ولفئات مختلفة من المجتمع تتناول الحديث عن هذه الجرائم.
- تصميم برامج في الإذاعة والتلفزيون تتناول شرح اساليب ومخاطر هذه الجرائم، ونشر بعض القصص الواقعية عنها.

[2] هناك خلافات كثيرة حول مشروع قانون العقوبات بين جهات كثيرة سواء الأحزاب السياسية أو المؤسسات والمنظمات الأهلية، وتعود هذه الخلافات إلى أن قانون العقوبات هو قانون على درجة كبيرة من الأهمية، ويشكل صمام الأمان للمجتمع، كما أن هذا القانون يقوم على مبدأ أن لا جريمة ولا عقوبة إلا بنص قانوني؛ ولذلك يصعب إقراره بموجب قرار بقانون إذ من المفروض أن يأخذ حقه الكامل في النقاش في المجلس التشريعي الفلسطيني. إضافة إلى ذلك هناك جدل كبير حول بعض العقوبات الهامة مثل عقوبة الإعدام بين من ينظر إليها على أنها جزء من العقيدة الإسلامية وبين من يريد إلغاؤها.

3- تصنيف الجرائم الإلكترونية وخصائصها وبعض الأمثلة عليها

يسلط هذا الجزء من الدراسة الضوء على تصنيف الجرائم الإلكترونية، وعلى بعض الأمثلة عليها في بعض الدول. ثم يبين أهم أنواع الجرائم الإلكترونية ومدى انتشارها في الأراضي الفلسطينية، وأسباب انتشارها، والإجراءات التي اتخذتها السلطة الفلسطينية للحد منها.

3-1 تصنيف الجرائم الإلكترونية

تصنف الجرائم الإلكترونية بشكل عام تبعاً لثلاثة تصنيفات (سمارة، 2008):

أولا- تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة:

- ✧ الجرائم التي تمس بقيمة معطيات الحاسوب.
- ✧ الجرائم التي تمس بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة.
- ✧ الجرائم التي تمس بحقوق الملكية الفكرية للبرامج الحاسوبية ونظمه (جرائم قرصنة البرمجيات).

ثانياً- تصنيف الجرائم تبعا لدور الحاسوب في الجريمة:

- ✧ الجرائم التي تستهدف عناصر السرية والسلامة ووفرة المعطيات والنظم، وتضم:
  - الدخول غير القانوني (غير المصرح به): حيث يقوم الشخص باختراق الشبكات والحواسيب التي ترتبط بشكبة الإنترنت، وذلك باختراق نظام الأمن في الشبكة والدخول إلى الجهاز والكشف عن محتوياته.
  - الاعتراض غير القانوني.
  - تدمير المعطيات (يكون هذا الأمر بعد اختراق الشبكة وقيام الشخص بمسح البيانات أو تشويها أو تعطيل البرامج المخزنة وجعلها غير قابلة للاستخدام).
  - اعتراض النظم.
  - إساءة استخدام أجهزة الحاسوب.
- ✧ الجرائم المرتبطة بالحاسوب وتضم: التزوير المرتبط بالحاسوب، والاحتيال المرتبط بالحاسوب.
- ✧ الجرائم المرتبطة بالمحتوى، وهي الجرائم المتعلقة بالأفعال الإباحية واللاأخلاقية.
- ✧ الجرائم المرتبطة بالإخلال بحق المؤلف وقرصنة البرمجيات.

ثالثاً- تصنيف الجرائم تبعا لمساسها بالأشخاص والأموال:

- ✧ جرائم الاحتيال والسرقة للمعلومات الإلكترونية المخزنة في أجهزة الحاسوب والمرسلة عبر الشبكات.
- ✧ الجرائم التي تستهدف الأشخاص: وهي الجرائم الجنسية، والجرائم غير الجنسية مثل التشهير والقدح والذم.
- ✧ جرائم الأموال (عدا السرقة) أو الملكية المتضمنة أنشطة الاختراق والإتلاف.

- ✧ جرائم التزوير: عملية التلاعب بالمعلومات المخزنة في الحاسوب، أو اعتراض المعلومات المرسلة بين الحواسيب المرتبطة بالشبكة، وذلك لغرض التضليل عن طريق تغييرها وتحريفها وتزويرها.
- ✧ جرائم المقامرة.
- ✧ جرائم الحاسوب المضادة للحكومة.

وكما يلاحظ فإن الحاسوب له صلة وثيقة بالجرائم الإلكترونية، وله دور أساسي وفعّال في مجال الجريمة الإلكترونية؛ فقد يكون الحاسوب هدفا للجريمة، أو أداة الجريمة لارتكاب جرائم تقليدية، أو بيئة الجريمة، كما هو الحال في تخزين البرامج المقرصنة فيه، أو في حالة استخدامه لنشر المواد غير القانونية. وقد يكون الحاسوب أداة في اكتشاف الجريمة.

2-3 خصائص الجرائم الإلكترونية

تختلف الجرائم الإلكترونية عن الجرائم التقليدية من مختلف النواحي، سواء من حيث أدوات الجريمة أو مكان وقوعها، أو شخصية مرتكبيها. وفيما يلي أهم خصائص هذه الجرائم:

2. عالمية الجريمة (جرائم عابرة للقارات): فهي لا تعرف الحدود السياسية والجغرافية بين الدول والقارات، فهي منتشرة بانتشار شبكة الإنترنت عبر العالم؛ ولذلك فقد يكون الجاني من دولة والمجني عليه من دولة أخرى، وكثيراً ما تحدث هذه الجرائم بين الأشخاص في أكثر من دولة.
3. جرائم صعبة الاثبات: فمن الصعوبة بمكان متابعتها واكتشافها، حيث أنها لا تترك أثراً فهي مجرد أرقام تتغير في السجلات. ولذلك، فإن معظم الجرائم الالكترونية تم إكتشافها بالصدفة وبعد وقت طويل من ارتكابها والجرائم التي لم تكتشف ربما أكبر بكثير من التي يتم الكشف عنها، لأنها تفتقر إلى الدليل المادي التقليدي كالبصمات وتحليل الخطوط والـــ DNA مثلا. وتعود صعوبة اكتشافها إلى الأسباب التالية:
   - ✧ أنها كجريمة لا تترك دليلاً مادياً يدل على مرتكبها.
   - ✧ صعوبة الاحتفاظ الفني بآثارها إن وجدت.
   - ✧ أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.
   - ✧ أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
   - ✧ أنها تعتمد على اتقان التعامل مع وسائل وادوات وبرامج تكنولوجيا المعلومات الحديثة في ارتكابها.
4. جرائم ناعمة: فهي تختلف عن الجريمة التقليدية في أنها لا تحتاج إلى مجهود عضلي في ارتكابها كالقتل، أو السرقة، أو الاغتصاب. حيث أنها تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي.
5. يلعب فرق التوقيت بين الدول، وكذلك البعد الجغرافي دوراً هاماً في تشتيت جهود البحث والتحري لتعقب هذه الجرائم.
6. تتسم هذه الجرائم بالغموض حيث يصعب إثباتها والتحقيق فيها كما هو الحال في الجرائم التقليدية.
7. عدم التبليغ عن كثير من الجرائم الإلكترونية بسبب خوف الضحية من التشهير.

خصائص الجناة في الجرائم الإلكترونية:

لكي نستطيع فهم الجاني في هذه الجرائم، لا بد من أن يوضع في الحسبان شخصية المجرم ومن أهم صفات التي توجد لدى بعضهم أو مجموعة منهم (الألفي، 2011):

- تتراوح أعمار مقترفي هذه الجرائم ما بين 18–46 عاماً.
- المعرفة والقدرة الفنية؛ فمعظمهم من أصحاب التخصصات ومستخدمي شبكة الإنترنت؛ ولديهم ثقة زائدة بالنفس تجعلهم يشعرون بإمكانية تنفيذ الجريمة دون أن يتم اكتشافها.
- يتمتعون بدرجة عالية من الذكاء تجعل من الصعب تصنيفه بحسب التصنيف الإجرامي المعتاد، لذا ينظر في تحديد أنواع الجناة في الجرائم الالكترونية إلى الهدف من ارتكابه لهذه الجرائم كمعيار للتميز فيما بينهم.
- الحرص الشديد والخوف من الضبط وافتضاح الأمر.
- القدرة على التخفي، فيظهر المجرم وكأنه من دول أخرى.
- إنسان اجتماعي ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على الحاسوب أو على البرامج التي يتم تشغيله بها.

3-3 بعض الأمثلة على الجرائم الإلكترونية

فيما يلي بعض الأمثلة على أشهر الجرائم الإلكترونية في بعض الدول:

- بينت دراسة لشركة سيمانتيك لأمن تكنولوجيا المعلومات في العام 2010 أن 65% من مستخدمي الانترنت في العالم كانوا ضحايا لجرائم الانترنت، ولو لمرة واحدة على الأقل، وأن نسبة كبيرة من مستخدمي الانترنت يشعرون بقلة الحيلة بعد هذه الجرائم، وحوالي 80% ممن خضعوا للدراسة لا يعتقدون أن الجناة في هذه الجرائم ستتم محاسبتهم. وأن 73% من مستخدمي الانترنت في الولايات المتحدة كانوا هدفا لفيروسات ضارة أو سرقة بيانات خاصة ببطاقاتهم الائتمانية أو انتحال شخصيات، وبلغت هذه النسبة في ألمانيا 62% (www.rosaonline.net).
- كشفت تحريات وكالة التحقيق الفدرالية الأمريكية في العام 2008 عن مليون حالة سرقة لأرقام بطاقات الائتمان الواردة في موقع 40 شركة أمريكية تمارس نشاطها عبر الإنترنت. وقد استخدموا الابتزاز مع الشركات وذلك: إما بنشر بيانات العملاء أو بدفع مبالغ نقدية كبيرة. ويعتقد أن معظم البيانات المسروقة بِيْعت لعصابات الجريمة المنظمة. ويصف مكتب التحقيقات الفدرالي هذه العملية بأنها أكبر عملية في تاريخ الشبكة (سمارة، 2008).
- في بريطانيا: جرى السطو على آلات الصرف الآلي ATM، مما أدى إلى خسائر بقيمة 15 مليون جنيه إسترليني من 33 ألف ماكينة خلال عام 2000 (سمارة، 2008).
- كشف تقرير أعده المكتب البريطاني لضمان أمن الإنترنت والمعلومات التابع لمجلس الوزراء بالتعاون مع مؤسسة "ديتكا " المتخصصة في تقنيات أمن المعلومات، أن الجرائم الإلكترونية تكلف الاقتصاد البريطاني نحو 27 مليار إسترليني سنوياً. تتأثر الحكومة والمواطنين بارتفاع معدلات الجرائم الإلكترونية بتقديرات تصل إلى 2.2 و3.1 مليار إسترليني على التوالي إلا أن المؤسسات التجارية تتحمل العبء الأكبر من التكلفة حيث تقدر

بنحو 21 مليار إسترليني. وأوضح التقرير أن سرقات حقوق الملكية الفكرية للمؤسسات التجارية هي الأكبر تأثيراً بتكلفة 9.2 مليار إسترليني، وأن أكثر القطاعات عرضة للهجمات الإلكترونية هي شركات الأدوية، وقطاعات التقنية الحيوية، والإلكترونيات، وتقنية المعلومات، والقطاعات العاملة في المجالات الكيماوية، وتأتي في المرتبة الثانية عمليات التجسس على الشركات والمؤسسات بتكلفة 7.6 مليار جنيه إسترليني، تليها جرائم الابتزاز بتكلفة 2.2 مليار جنيه إسترليني، وتأتي بعدها جرائم السرقة المباشرة على الإنترنت والتي تكلف الشركات والمؤسسات 1.3 مليار إسترليني، منها حوالي مليار جنيه إسترليني عبارة عن خسائر تتعلق بسرقة معلومات وبيانات العملاء. وتشمل الخسائر السنوية التي يتكبدها المواطنون البريطانيون جراء الجرائم الإلكترونية نحو 1.8 مليار جنيه إسترليني لانتحال الشخصية و1.4 للاحتيال عبر شبكة الإنترنت (www. omarsalloum.7olm.org).

- تمكنت السلطات الأمريكية من إيقاف عمل عصابة الكترونية جمعت أكثر من 72 مليون دولار أمريكي عن طريق بيع برامج حماية وهمية لمستخدمي الانترنت، حيث توحي بوجود مخاطر أمنية تهدد أجهزة الكمبيوتر ثم تطلب من المستخدمين شراء هذه البرامج لإصلاح أي مشاكل وهمية داخل هذه الأجهزة، وقد قام أن أكثر من مليون شخص بتثبيت البرامج الوهمية على أجهزتهم ودفعوا 129 دولار أمريكي ثمنا للنسخة الواحدة، وتعرضت أجهزة الحاسوب الخاصة بالذين قاموا بتنزيل البرامج ولم يدفعوا ثمنا إلى هجمات من الرسائل تحذرهم من المخاطر التي تهدد أجهزتهم. وذلك بعد أن قامت السلطات بسلسلة من المداهمات بالتنسيق مع مكتب التحقيقات الفيدرالي في الولايات المتحدة وبريطانيا وست دول أخرى. وتم ضبط 40 جهاز حاسوب استخدمت في عمليات مسح وهمية والصفحات الالكترونية على شبكة الانترنت التي خدعت المستخدمين وأغرتهم لشراء برامج الحماية الوهمية. وأسفرت حملة المداهمات التي وقعت في لاتفيا عن استعادة الشرطة هناك السيطرة على خمسة حسابات مصرفية استخدمتها العصابة لجمع النقود (www.bbc.co.uk).
- تشهد بريطانيا جريمة إلكترونية جديدة كل 10 ثوان، حيث تم ارتكاب أكثر من 3 ملايين جريمة إلكترونية خلال العام 2006 تراوحت هذه الجرائم بين الحصول على معلومات شخصية حول مستخدمي الإنترنت، والتحرش الجنسي بهم، وممارسة الاحتيال عبر شبكة الإنترنت (www.moheet.com).
- أظهر استطلاع للرأي أجراه تلفزيون "أم تي في" أن 56% من المشاركين في الاستطلاع خلال العام 2010 الذين تتراوح أعمارهم بين 14–24 سنة أنهم تعرضوا لسوء المعاملة من خلال وسائل الإعلام الرقمية، تمثلت بالتخويف أو المضايقة أو التحرش (جريدة القدس، 2011).

أما أبرز الهجمات الإكترونية في العام 2010 فهي (www.emaratalyoum.com):

- نظام سيبرنت وتسريبات ويكليكس: نظام سيبرنت هو نظام لتبادل المعلومات بين وزارة الخارجية ووزارة الدفاع الأمريكية لتبادل الوثائق وأرشفتها، وباستطاعة آلاف الأشخاص مشاهدة تلك الوثائق كل شخص حسب اختصاصه أو رتبته، بمعنى أن الضباط والموظفين الكبار بإمكانهم مشاهدة أكبر عدد من الوثائق مقارنة بصغار الضباط والموظفين. ويعتقد أن الوثائق التي سربها موقع ويكيليكس لم يجر تصنيفها، أو أنها اعطيت تصنيفات منخفضة، بحيث أتيحت للمطالعة من قبل أشخاص غير معنيين. ويحتوي نظام سيبرنت على مرجع للأشخاص الذين دخلوا إليه مع التاريخ والوقت والفترة التي قضوها في النظام، وبالتالي من السهولة ضبط المتسللين. ولذلك فإن السبب الرئيس لتسريب الوثائق ضعف الرقابة الأمنية على نظام سيبرنت.

- ✧ فيروس ستوكسنت: يصيب هذا الفيروس أجهزة الحاسوب العاملة ضمن أنظمة التحكم الصناعية، ويقوم بأعمال تجسس على هذه الأنظمة ويعمل على إعادة برمجتها، إذ تمت برمجته خصيصاً للهجوم على أنظمة (سكادا) المخصصة للمراقبة والتحكم وتجميع البيانات. وهناك تقديرات بأن الفيروس أصاب نحو 45 ألف حاسب آلي في أنحاء العالم في إيران، وإندونيسيا، والولايات المتحدة الأمريكية.
- ✧ فيروس زيوس: يستهدف هذا الفيروس الحسابات المصرفية على الإنترنت، إذ يسرق البيانات المسجلة على الإنترنت عن طريق اختراق المستخدم الذي يكون في قائمة المواقع المستهدفة. وظهر خلال العام 2010 نسخة مطوّرة من الفيروس تؤدي إلى زيادة الخسائر الناجمة عن الاحتيال وتستهدف ثغرة أمنية في متصفح فاير فوكس، إذ كشفت دراسات أن نحو 30٪ من مستخدمي الإنترنت يجرون عملياتهم المصرفية على الإنترنت من خلال متصفح فاير فوكس. ويشار إلى أن الإصابة بـــهذا الفيروس تنمو بصورة متسارعة. وتصدرت مصر والسعودية عالمياً قائمة أكثر الدول إصابة بهذا الفيروس.
- ✧ فيروس زومبي: يستهدف هذا الفيروس الهواتف النقالة، إذ يتحد مع التطبيق الأمني على الهاتف، ثم ينقل بعد ذلك تفاصيل بطاقة الهاتف إلى برنامج مركزي تسيطر عليه مجموعة صغيرة من القراصنة، وضرب الفيروس أكثر من مليون جهاز هاتف محمول في الصين وحدها، وهو ينتقل من هاتف إلى آخر. وقد انحصر انتشاره في الأجهزة المصنعة في الصين، ولكن على الرغم من ذلك، فإن المخاوف تبقى من ظهور نسخ إضافية أو مطوّرة منه تؤثر في الأجهزة النقالة أو الذكية منها في بلدان أخرى.
- ✧ رسائل التصيد: يستخدم مرسلو هذه الرسائل برامج خاصة لتغيير اسم مرسل الرسائل، وغالباً ما يستخدمون اسم بنك معين أو موقع مشهور ويطلبون من الشخص التسجيل في الموقع، أو إعطاء الشخص برنامجاً جديداً للتجربة ولعمل تنظيف لجهاز الحاسوب، ويكون الشخص بهذه الحالة ضحية لتلك الهجمات. وهذه الرسائل تصل عبر البريد الإلكتروني وتحمل برامج خبيثة هدفها التجسس لحساب المرسل، للإيقاع بالمستخدمين وسرقة بياناتهم الشخصية وأرقام حساباتهم عن طريق إرسال رسائل تحتوي على عروض استثمارية ضخمة وثروات من الذهب وما شابه.

4- مقارنة أحكام الجرائم الإلكترونية مع القوانين السارية

يسلط هذا الجزء من الدراسة الضوء على الواقع القانوني في الأراضي الفلسطينية من حيث مدى معالجته للجرائم الإلكترونية، ومقارنة الأحكام المتعلقة بالجرائم الإلكترونية مع أحكام القوانين الأخرى ومدى انسجامها معها.

4-1 القانون الأساسي المعدل لسنة 2003:

بالاطلاع على القانون الأساسي المعدل لسنة 2003 يتضح أن النصوص المتعلقة بالجرائم الإلكترونية تنسجم مع ما ورد في القانون الأساسي. وتجدر الإشارة هنا إلى أن القانون الأساسي قد كفل الحرية الشخصية وكرامة الفرد، ولكنه بالمقابل لا يسمح باعتقال شخص دون أمر قضائي، أو معاقبته على فعل ما دون نص قانوني. فالمادة 1/11 من القانون الأساسي بينت أن الحرية الشخصية حق طبيعي وهي مكفولة لا تمس. كما بينت مادة 32 أن كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي أو القانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع عليه الضرر.

كما بينت المادة 2/11 أنه لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد أو منعه من التنقل إلا بأمر قضائي وفقاً لأحكام القانون، ويحدد القانون مدة الحبس الاحتياطي، ولا يجوز الحجز أو الحبس في غير الأماكن الخاضعة للقوانين الصادرة بتنظيم السجون، كما بينت المادة 12 أنه يجب تبليغ كل من يقبض عليه أو يوقف بأسباب القبض عليه أو إيقافه، ويجب إعلامه سريعاً بلغة يفهمها بالاتهام الموجه إليه، وأن يمكنه من الاتصال بمحام، وأن يقدم للمحاكمة دون تأخير. كما أكدت المادة 14 أن المتهم برئ حتى تثبت إدانته في محاكمة قانونية تكفل له فيها ضمانات الدفاع عن نفسه، وكل متهم في جناية يجب أن يكون له محام يدافع عنه.

من ناحية أخرى بينت المادة 117 أنه لا تسري أحكام القوانين إلا على ما يقع من تاريخ العمل بها، ويجوز عند الاقتضاء في غير المواد الجزائية النص على خلاف ذلك.

4-2 قانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية

ناقش هذا القانون الجوانب المتعلقة بالاتصالات السلكية واللاسلكية، حيث أنه بموجب هذا القانون تكون ملكية قطاع الاتصالات السلكية واللاسلكية للسلطة الوطنية الفلسطينية وتخضع للأحكام المنصوص عليها فيه، ويجوز لمجلس الوزراء أن يمنح حق امتياز أو أكثر في قطاع الاتصالات السلكية واللاسلكية، وأن يقرر حصر الاتصالات أو تعليقها إذا اقتضى الأمن الوطني أو مصالح أخرى جوهرية ذلك. ولا يترتب من جراء ذلك دفع أي عطل أو ضرر أو تعويض أو إعادة البدلات. كما بينت المادة 4 أن سرية الاتصالات على الأراضي الفلسطينية مصونة ولا يجوز المس بها إلا للسلطة العامة وحدها وفي حدود القانون، ثم بين المهام التي تطلع بها وزارة الاتصالات وتكنولوجيا المعلومات، من حيث الإشراف والرقابة ومنح التراخيص في هذا القطاع، وتنظيم قطاع الاتصالات في السلطة بما يواكب تطور تكنولوجيا الاتصالات وحماية مصالح المستفيدين من خدمات الاتصالات، ومراقبة أداء الجهات

المرخصة لتقديم خدمات الاتصالات، واتخاذ الإجراءات اللازمة لإلزام تلك الجهات بالتقيد بشروط الترخيص، بما في ذلك نوعية ومستوى الخدمات والعمل على تطويرها.

ويتبين أن القانون لم يتطرق لموضوع الجرائم الإلكترونية، كما أنه لم ينظم آلية الاتصال بالإنترنت، وبالمحصلة فإن الأحكام المتعلقة بالجرائم الإلكترونية لم تعالج في قانون الاتصالات.

4-3 قانون العقوبات رقم 16 لسنة 1960

تناول قانون العقوبات كافة أنواع الجرائم، وحدد العقوبة الملائمة لكل منها، ولكن نظراً لقدم القانون فإنه لم يشر إلى استخدام وسائل الاتصال الحديثة في ارتكاب هذه الجرائم، وإن كان قد نص على تجريم ارتكاب جرائم القدح أو الذم أو التشهير او السرقة والنصب والاحتيال وغيرها التي تمارس على نطاق متزايد بواسطة الوسائل الالكترونية. ومن بعض الأمثلة على ما جاء في قانون العقوبات ما يلي:

- بينت المادة 213 أن من ثبت انتحاله اسم غيره في تحقيق قضائي أو محاكمة قضائية عوقب بالحبس من شهر إلى سنة.
- بينت المادة 348 أنه يعاقب بالحبس مدة لا تتجاوز الأسبوع أو بغرامة لا تتجاوز العشرة دنانير من تسلل بواسطة الكسر أو العنف على الأشخاص إلى أماكن تخص الغير وليست مباحة للجمهور، أو مكث فيها على الرغم من إرادة من له الحق في إقصائه عنها. ولا يلاحق المجرم إلا بناء على شكوى الفريق المتضرر.
- عرفت المادة 399 السرقة بأنها أخذ مال الغير المنقول دون رضاه. وتعني عبارة (أخذ المال) إزالة تصرف المالك فيه برفعه من مكانه ونقله وإذا كان متصلاً بغير منقول فبفصله عنه فصلاً تاماً ونقله. تشمل لفظة (مال) القوى المحرزة.
- نصت المادة 416 على معاقبة كل من استعمل دون حق شيئاً يخص غيره بصورة تلحق به ضرراً دون أن يكون قاصداً اختلاس ذلك الشيء، بالحبس حتى ستة أشهر، وبالغرامة حتى عشرين ديناراً أو بإحدى هاتين العقوبتين.
- نصت المادة 445 على معاقبة كل من ثبت الحقاه ضرراً بمال غيره المنقول باختياره، وبناء على شكوى المتضرر، بالحبس مدة لا تتجاوز سنة أو بغرامة لا تتجاوز خمسين ديناراً أو بكلتا العقوبتين. وأن تنازل المشتكي (..) يسقط دعوى الحق العام.

ويتضح مما سبق أن جميع الأفعال التي يجرمها قانون العقوبات، قد تحدث في زماننا الحاضر ولكن من خلال الوسائل الإلكترونية، وهو ما تحاول الأحكام المتعلقة بالجرائم الإلكترونية تنظيمه، وفرض العقوبة الملائمة على كل منها.

4-4 قرار بقانون رقم (9) لسنة 2007 بشأن مكافحة غسل الأموال

عرف القرار بقانون غسل الأموال: كل سلوك يقصد به إخفاء أو تغيير هوية الأموال المتحصلة من إحدى الجرائم الأصلية وذلك تمويهاً لمصادرها الحقيقية لتبدو في ظاهرها متأتية من مصادر مشروعة.

حدد القرار بقانون الأفعال التي تعد جريمة غسل الأموال وهي استبدال أو تحويل الأموال التي تكون متحصلات جريمة أو إخفاء أو تمويه الطبيعة الحقيقية لهذه الأموال، أو تملك الأموال أو حيازتها أو استخدامها مع العلم أن هذه الأموال هي متحصلات جريمة. أو الاشتراك أو المساعدة أو التحريض أو التآمر أو تقديم المشورة أو النصح أو التسهيل أو التواطؤ أو التستر أو الشروع في ارتكاب أي من الأفعال السابقة. كما يعد مالاً غير مشروع ومحلا لجريمة غسل الأموال كل مال متحصل من أي من الجرائم التالية: 1. المشاركة في جماعة إجرامية وجماعة نصب منظمة. 2. الاتجار في البشر وتهريب المهاجرين. 3. الاستغلال الجنسي للأطفال والنساء. 4. الاتجار غير المشروع في العقاقير المخدرة والمؤثرات العقلية. 5. الاتجار غير المشروع في الأسلحة والذخائر. 6. الاتجار غير المشروع في البضائع المسروقة وغيرها. 7. الرشوة والاختلاس. 8. الاحتيال. 9. تزوير العملة والوثائق الرسمية. 10. التزوير، والاعتداء على الملكية الفكرية. 11. الجرائم التي تقع مخالفة لأحكام قانون البيئة. 12. القتل أو الإيذاء البليغ. 13. الخطف أو الاحتجاز أو أخذ الرهائن. 14. السطو والسرقة. 15. التهريب. 16. الابتزاز أو التهديد أو التهويل. 17. التزوير. 18. القرصنة بشتى أنواعها. 19. التلاعب في أسواق المال. 20. الكسب غير المشروع.

أوجب القانون على تجار المعادن الثمينة وتجار الأحجار الكريمة والتجار الآخرين الذين يتعاملون في الصفقات ذات القيمة العالية والمؤسسات المالية والأعمال والمهن غير المالية التعرف على عملائهم. وفي حالة الاشتباه في أن الأموال تمثل متحصلات جريمة، أو كان لديهم علما بواقعة أو نشاط قد يشكل مؤشراً على جريمة غسل الأموال، أن تقدم تقارير بذلك على وجه السرعة إلى وحدة المتابعة المالية ، وفقا للتعليمات التي تصدرها الوحدة بهذا الشأن.

ناقش القرار بقانون ما يتعلق باللجنة الوطنية لمكافحة جريمة غسل الأموال من حيث آلية تشكيلها واختصاصاتها وآلية اتخاذ القرارات فيها. ثم ناقش ما يتعلق بوحدة المتابعة المالية وهي وحدة مستقلة لمكافحة جريمة غسل الأموال تشكل مركز معلومات وطني ومقرها سلطة النقد وحدد القانون اختصاصاتها.

أما العقوبات التي فرضها القرار بقانون لمخالفة أحكامه فقد تراوحت بالحبس ما بين 1–15 سنة، أو بغرامة مالية من 5–100 ألف دينار، أو بكلتا هاتين العقوبتين، ويتضاعف الحد الأعلى للغرامة إذا كان الشخص اعتباريا. أما عقوبة الشروع بارتكاب جريمة غسل الأموال أو المساعدة أو التحريض أو تسهيل أو التشاور حول ارتكاب هذه الجريمة بنصف العقوبة التي يعاقب بها الفاعل الأصلي. كما يحكم بالمصادرة العينية لمتحصلات الجريمة، وتصبح الأموال المصادرة من حق السلطة الوطنية وتسري بشأنها القوانين السارية. وعلى مجلس الوزراء إصدار اللوائح اللازمة لتنفيذ أحكام هذا القانون بتنسيب من اللجنة الوطنية خلال سنة من تاريخ صدور هذا القانون (2007/10/25).

تجدر الإشارة إلى أن هناك انتقادات كبيرة لهذا القرار بقانون[3] وأن الهدف من إصداره سياسي لمكافحة ما يسنى بالإرهاب ولكن ليس هنا محل نقاشها. وبالاطلاع على القرار بقانون وبالمقارنة مع الأحكام المتعلقة بالجرائم الإلكترونية يمكن توضيح الأمور التالية:

[3] لمزيد من التفاصيل أنظر: الائتلاف من أجل النزاهة والمساءلة (أمان)، 2009. **سلسلة تقارير (20) الواقع التشريعي مراجعة نقدية للقرار بقانون لسنة 2007 بشان غسيل الأموال**. رام الله–فلسطين.

- على الرغم من حداثة القرار بقانون بشأن مكافحة غسيل الأموال حيث صدر في نهاية العام 2007 تقريباً، إلا أنه لم يشر إلى استخدام الوسائل التكنولوجية في ارتكاب جرائم غسيل الأموال مع أنها قد تكون الوسائل الأكثر استخداماً لتنفيذ الجرائم المذكورة أعلاه. خاصة وأن القانون قد أشار إلى موضوع الوسائل التكنولوجية في أكثر من مادة. فعلى سبيل المثال عرف في المادة 1 التحويل البرقي[4] كما أشار في المادة 8 إلى التحويلات الإلكترونية أيضاً. ولذلك، فإن الأحكام المتعلقة بالجرائم الإلكترونية تأتي مكملة للقرار بقانون بشأن مكافحة غسيل الأموال.
- تشير بعض الدراسات إلى انتشار جرائم غسيل الأموال في الأراضي الفلسطينية وقدرتها بنحو 300 مليون دولار سنوياً (عبد الكريم، 2008)، الأمر الذي يتطلب اشتمال قانون الجرائم الإلكترونية لدى صياغته على الجرائم المتعلقة بغسيل الأموال كما سيرد تفصيله لاحقاً.
- حدد القرار بقانون عقوبات رادعة لمخالفة أحكامه كما سبق ذكره، وهي عقوبات عالية نسبياً مقارنة بالعقوبات المفروضة بموجب أحكام مشروع قانون العقوبات بما في ذلك ما ورد في مشاريع قوانين أخرى تناولت المعاملات الإلكترونية.

4-5 قوانين أخرى نصت أحكامها على استخدام الوسائل التكنولوجية في عملياتها، أو لطرق الإثبات فيها. مثل:

- قرار بقانون رقم 9 لسنة 2010 بشأن المصارف، ورد في المادة 13 أن من ضمن الأعمال المصرفية المسموح بها إصدار وإدارة وسائل الدفع، بما في ذلك البطاقات الدائنة والمدينة. كما بينت المادة 6/46 أنه يجوز الإثبات في القضايا المصرفية بجميع طرق الإثبات بما في ذلك البيانات الإلكترونية أو البيانات الصادرة عن النظام الآلي للمصرف.

كما فرضت المادة 54 على كل من يخالف أحكام القانون والأنظمة والتعليمات والقرارات الصادرة بموجبه غرامة مالية لا تقل عن 5 آلاف دولار أمريكي ولا تزيد على 250 ألف دولار أمريكي أو ما يعادلها من العملات المتداولة في فلسطين، وما يتبع ذلك من مسؤولية مدنية أو جزائية وفقاً لأحكام أي تشريع آخر.

يتضح من النص السابق الاعتماد على الوسائل التكنولوجية في عمل المصارف، وكذلك استخدامها في الإثبات في القضايا المصرفية. ولا يخفى مدى انتشار البطاقات الإلكترونية في عمل المصارف مما يزيد من احتمالية ارتكاب الجرائم الإلكترونية بواسطتها، ولكن قانون المصارف لم يحدد عقوبة سرقة بطاقة الصراف الآلي واستخدامها لسحب رصيد لشخص آخر، ولكن حدد عقوبة عالية لمخالفة أحكام القانون أو الأنظمة والتعليمات الصادرة بمقتضاه، وهي عقوبة عالية جداً مقارنة بالعقوبات المفروضة بموجب أحكام مشروع قانون العقوبات أو المعاملات الإلكترونية.

- قانون الأوراق المالية رقم 12 لسنة 2004، حيث بينت المادة 19 أنه تعتبر قيود سجلات مركز الإيداع والتحويل والتسوية وحساباته وأية مستندات يدوية أو الكترونية صادرة بموجبها بينة، ما لم يثبت عكس ذلك.

[4] أية عملية يجري تنفيذها بالنيابة عن الشخص (سواء كان طبيعياً أو اعتبارياً) من خلال مؤسسة مالية عن طريق وسيلة إلكترونية بهدف توفير مبلغ من المال لصالح شخص مستفيد في مؤسسة مالية أخرى.

كما أعطت المادة 26 الحق لهيئة سوق رأس المال أن تحدد صيغة أو شكلا معينا للتوقيع الإلكتروني لاعتماده يكون مساويا في حجيته للتوقيع الخطي.

كما حددت المادة 100 العقوبـــات المفروضة في حالة مخالفة أحكام القانون أو اللوائح أو التعليمات أو الأنظمة الصادرة بمقتضاه بأن يغرم بما لا تزيد على 100 ألف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو الحبس مدة لا تزيد عن سنة أو بكلتا هاتين العقوبتين، بالإضافة إلى إلزام الشخص المخالف بإعادة الربح الذي حققه أو تضمينه قيمة الخسارة التي وقعت على الغير.

بينت المادة 2/101 أنه على الرغم مما ورد في أي تشريع آخر، فإنه يجوز الإثبات بقضايا الأوراق المالية والمعاملات التي تتم لدى الهيئة والسوق بواسطة البيانات الإلكترونية أو الصادرة عن الحاسوب وتسجيلات الهاتف ومراسلات أجهزة التلكس والفاكسميلي.

يتضح أيضاً من النص السابق الاعتماد على الوسائل الإلكترونية في التداول بالأوراق المالية، وكذلك استخدام الوسائل الالكترونية في الإثبات في قضايا الأوراق المالية. كما أن هناك نظام إلكتروني للتداول بالأوراق المالية، مما يعني احتمالية كبيرة لارتكاب الجرائم الإلكترونية من خلال هذه المعاملات، وقد حدد القانون سقفاً عالياً للعقوبة المفروضة على مخالفة قانون الأوراق المالية أو الأنظمة والتعليمات الصادرة بمقتضاه مقارنة بالعقوبات المفروضة بموجب أحكام مشروع قانون العقوبات أو المعاملات الإلكترونية.

4-6 قرارات مجلس الوزراء ذات العلاقة بشأن الإنترنت، والتي أهمها:

- ✧ قرار مجلس الوزراء رقم (3) لسنة 2004 الصادر بتاريخ 2004/1/26، بشأن منع بيع وتسويق خدمات الاتصالات وتقنية المعلومات والبريد السريع، وبموجبه يمنع بيع وتسويق خدمات الاتصالات وتقنية المعلومات والبريد السريع غير المرخصة من جهات الاختصاص في مناطق السلطة الوطنية الفلسطينية. وتتولى وزارة الداخلية ووزارة العدل وبالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات متابعة تنفيذ هذا القرار.
- ✧ قرار مجلس الوزراء رقم 34 لسنة 2004 بشأن إنشاء الشبكة الحكومية المستقلة للاتصالات، صدر بتاريخ 2004/1/26، وتنشأ بموجبه الشبكة الحكومية المستقلة للاتصالات وتكلف وزارة الاتصالات وتكنولوجيا المعلومات بالبدء بإعداد الدراسات الفنية اللازمة لذلك.
- ✧ قرار مجلس الوزراء رقم 35 لسنة 2004 بشأن النفاذ إلى الشبكة العالمية (الإنترنت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي، صدر بتاريخ 2004/1/26. حيث تلتزم وزارة الاتصالات والتكنولوجيا بتوفير خدمة النفاذ إلى الشبكة العالمية (الإنترنت) واستخدام البريد الإلكتروني إلى المؤسسات والدوائر الحكومية من خلال الخدمات التي يوفرها مركز الحاسوب الحكومي وإتاحتها على أساس تميز هذه الخدمات بالحداثة والسرعة والكفاءة ونجاعة الحماية من الاختراق الخارجي والصيانة والمنافسة محليا. وتلتزم الوزارات والمؤسسات والدوائر الحكومية بالنفاذ إلى الشبكة العالمية (الإنترنت) واستخدام البريد الإلكتروني من خلال الخدمات التي يوفرها مركز الحاسوب الحكومي. ويجوز لأي من الوزارات والمؤسسات والدوائر الحكومية طلب الخدمة من خارج مركز الحاسوب الحكومي إذا تميزت هذه الخدمة علميا أو تقنيا أو من حيث سرعة النفاذ والحماية من الاختراق الخارجي عن تلك المتوافرة في مركز الحاسوب الحكومي. لا تعتمد أية تكاليف أو

نفقات خاصة بخدمات تتلقاها الوزارات والمؤسسات والدوائر الحكومية التي تتم خارج مركز الحاسوب الحكومي في مجال النفاذ إلى الشبكة العالمية (الإنترنت) واستخدام البريد الإلكتروني، إذا كانت هذه الخدمات متوافرة ومتاحة بالكفاءة والمنافسة محليا في مركز الحاسوب الحكومي.

- ✧ قرار مجلس الوزراء رقم 65 لسنة 2005 صدر بتاريخ 2005/5/10 بالمصادقة على اعتماد مبادرة فلسطين الإلكترونية (E-Palestine) بجميع مكوناتها المتمثلة في: الحكومة الإلكترونية، والتعليم الإلكتروني، والبطاقة الذكية، والمعهد القومي للاتصالات وتكنولوجيا المعلومات، ودعم دور المرأة في قطاع الاتصالات وتكنولوجيا المعلومات، ومشروع الشراكة الفلسطينية – الأورومتوسطية، ومبادرة التعليم الإلكتروني، ومشروع تراث لحوسبة المخزون الفكري الفلسطيني. وبموجب القرار تقوم اللجان الوزارية واللجان الإشرافية ولجان العمل والتنسيق المنبثقة عن اللجان الوزارية بمتابعة كافة المهام لإنجاز مبادرة فلسطين الإلكترونية من خلال إعداد النظام واللوائح الداخلية والبنية الهيكلية والدراسات المسحية وحملات التوعية، واعتماد المشاريع اللازمة لتنفيذ خطوات المبادرة وتقديمها إلى الدول المانحة لتجنيد الدعم اللازم للمبادرة وتنفيذه بالتعاون مع الوزارات المعينة والمؤسسات والهيئات الفلسطينية ذات العلاقة وبالشراكة مع القطاع الخاص والأكاديمي ومؤسسات العمل والمنظمات غير الحكومية. ويكون وزير الاتصالات والتكنولوجيا مقرراً لعمل اللجان المنبثقة عن المبادرة الفلسطينية ويقدم توصياته إلى مجلس الوزراء لاتخاذ القرارات المناسبة.
- ✧ قرار مجلس الوزراء رقم 74 لسنة 2005 بشأن الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات، صدر بتاريخ 2005/5/18. تُعتمد الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات كاستراتيجية وطنية بهدف وضع الخطوط العريضة والمحاور العامة التي تنظم جهود المجتمع الفلسطيني لتطوير مجتمع المعلومات لكي يلعب دوراً فاعلاً في تحقيق التنمية الشاملة في فلسطين. وعلى وزارة الاتصالات وتكنولوجيا المعلومات التعاون والتنسيق مع كافة الأطراف الرئيسية في المجتمع الفلسطيني على الصعيد الحكومي والقطاع الخاص ومؤسسات المجتمع المدني والجامعات، لوضع الاستراتيجية الوطنية موضع التنفيذ من خلال العمل على تأمين البنية الأساسية للمعلومات والاتصالات (الاستثمار والتمويل، الإتاحة والتنمية، الاستمرارية والشراكة الأوسع في الاستثمار) مع المراجعة الدائمة والتقييم لما يتم إنجازه. وعلى وزارة الاتصالات والتكنولوجيا التعاون مع الأطراف ذات الصلة من خلال رسم خطوط واضحة لما يلزم من سياسات وتشريعات وآليات للتحكم في قطاع الاتصالات وتكنولوجيا المعلومات وتحريره واندماجه في اقتصاد السوق الحر. تقوم وزارة الاتصالات وتكنولوجيا المعلومات بإطلاق حملة وطنية للوعي الإلكتروني في منافع تكنولوجيا الاتصالات والمعلومات للمجتمع الفلسطيني، وإضافة بعد جديد عن الوعي الإلكتروني لمختلف تطبيقات تكنولوجيا الاتصالات والمعلومات وبرامجها.
- ✧ قرار مجلس الوزراء رقم 269 لسنة 2005 بالمصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة صدر في 2005/10/20.

1. المصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة المتمثلة في: الحواسيب الموجودة في الوزارات والمؤسسات العامة كافة، وشبكة الإنترنت المتاحة في تلك المؤسسات، هي ملك للسلطة الوطنية الفلسطينية وتعتبر ملكاً عاماً وليس ملكاً شخصياً.
2. تتولى الإدارات والدوائر والأقسام المختصة في المؤسسات العامة أو من تتعاقد معه تركيب وصيانة هذه الحواسيب وشبكة الإنترنت وليس لأحد سواها أحقية القيام بهذه الأعمال دون الحصول على موافقة على

هذه الجهات، وفي كل الأعمال المرتبطة بتشغيل وتطوير وتبديل وإدخال تقنيات جديدة تستوجب العودة إلى تلك الجهات.

3. توظيف التقنيات الحديثة المتاحة كافة، لمصلحة العمل والحفاظ على المال العام وأمن المعلومات وجودة الخدمات.
4. حظر استخدام هذه التقنيات بما يتنافى مع التعاليم الدينية والعادات والتقاليد والحياء العام أو استخدامها لأغراض الترفيه أو ارتياد المواقع الإباحية ومواقع القمار والألعاب الإلكترونية، أو استجلاب برمجيات غير قانونية، أو ما هو خارج عن نطاق عمل تلك المؤسسات تحت طائلة المسئولية القانونية.

- ✧ قرار مجلس الوزراء رقم 276 لسنة 2005 بشأن تفعيل مركز الحاسوب الحكومي صدر بتاريخ 2005/10/27. تخصيص مبلغ 244 ألف دولار أمريكي منها 10 آلاف دولار أمريكي دفعة مرة واحدة، والباقي يدفع سنوياً لاستبدال خطوط شبكة الحاسوب (الانترنت) الحالية التي لم تعد تتلاءم مع المتطلبات العصرية للتكنولوجيا.

ويلاحظ أن كافة هذه القرارات لم تتطرق إلى الجرائم الإلكترونية، باستثناء ما اشار إليه القرار رقم 269 الذي يحظر على موظفي المؤسسات العامة استخدام الإنترنت بما يتنافى مع التعاليم الدينية والعادات والتقاليد وغيرها، ولكن القرار لم يشر إلى العقاب على هذا الفعل في حال ارتكابه.

5- مقارنة النصوص المتعلقة بالجرائم الإلكترونية مع قوانين بعض الدول الأخرى

يتناول هذا الجزء من الدراسة مقارنة النصوص المتعلقة بالجرائم الإلكترونية والتي وردت في مشروعي قانوني العقوبات والمعاملات الإلكترونية، مع قوانين بعض الدول الأخرى بهدف الاستفادة من تجارب هذه الدول في تطوير هذه النصوص أو تطوير مشروع قانون يعالج الجرائم الإلكترونية في الأراضي الفلسطينية. وستتم هذه المقارنة وفقاً لخمسة معايير: إذ سيتم في البداية التعرف على الإطار القانوني الذي يتعامل مع هذه الجرائم في الدول الأخرى، ثم سيتم مقارنة الجرائم الواردة في مشروعي القانونين مع قوانين الدول الأخرى، ومدى تشدد أو تساهل المشرع الفلسطيني في العقوبات المفروضة على هذه الجرائم بالمقارنة مع الدول الأخرى، ثم الاستفادة من تجارب هذه الدول فيما إذا نصت على جرائم أخرى لم ترد في مشروعي القانونين، أو إجراءات أخرى لم يذكرها المشرع الفلسطيني.

5-1 الإطار القانوني لمعالجة الجرائم الإلكترونية

كما سبق القول فإن النصوص المتعلقة بالجرائم الإلكترونية قد وردت في كل من مشروع قانون العقوبات ومشروع قانون المعاملات الإلكترونية، ولكن بالنظر إلى قوانين الدول الأخرى يتبين أنها سنت قانوناً خاصاً بالجرائم الإلكترونية. مثل: قانون جرائم أنظمة المعلومات قانون مؤقت لسنة 2010 في الأردن، والقانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات في الإمارات، وقانون جرائم المعلوماتية لسنة 2007 في السودان، ومرسوم سلطاني رقم 2011/12 بإصدار قانون مكافحة جرائم تقنية المعلومات في عمان، وقانون العقوبات القطري رقم 11 لسنة 2004 ورد به فصل جرائم الحاسب الآلي المواد، وقانون البيانات الشخصية رقم 204 لسنة 1998 في السويد، وقانون جرائم الكمبيوتر والجريمة السيبرانية رقم 22 لسنة 2003 في اليابان. واتفاقية بودابست للجرائم الإلكترونية الموقعة في 2001/11/23 بين دول الاتحاد الأوروبي.

ومن هنا واستفادة من تجارب الدول الأخرى، يجدر تجميع النصوص المتعلقة بالجرائم الإلكترونية في مشروع قانون واحد يسمى مشروع قانون الجرائم الإلكترونية كما هو الحال في قوانين معظم الدول. يتشابه القانون السوري وهو قانون التوقيع الإلكتروني وخدمات الشبكة لسنة 2009 مع مشروع قانون المعاملات الإلكترونية، أما القانون القطري فقد أورد وأسهب في تفصيل ما يتعلق بالجرائم الإلكترونية في قانون العقوبات. أما في عمان فهناك قانون للمعاملات الإلكترونية وقانون آخر للجرائم الإلكترونية، كما ألغى قانون الجرائم الإلكترونية الفصل المتعلق بالجرائم الإلكترونية في قانون الجزاء العماني.

5-2 أنواع الجرائم الإلكترونية

حسب مشروع قانون العقوبات تنقسم الجرائم وفقاً لجسامتها إلى جنايات وجنح ومخالفات، ويحدد نوع الجريمة بنوع العقوبة الأشد المقررة لها في القانون، وإذا اجتمع في عقوبة جريمة ما الحبس والغرامة فيحدد نوع الجريمة بمقدار عقوبة الحبس المقررة لها:

- الجنايات هي الجرائم المعاقب عليها بالعقوبات التالية: السجن مدى الحياة، أو السجن المؤبد لمدة عشرين سنة، أو السجن المؤقت الذي لا تقل مدته عن 3 سنوات ولا تزيد على 15 سنة، ما لم ينص القانون على خلاف ذلك.
- الجنح هي الجرائم المعاقب عليها بالعقوبات التالية: الحبس الذي لا تزيد مدته عن 3 سنوات، أو الغرامة التي تتراوح بين 100–500 دينار أردني إلا إذا نص القانون على خلاف ذلك، أو العمل للمصلحة العامة.
- المخالفات هي الجرائم المعاقب عليها بالغرامة التي لا تجاوز 100 دينار أردني.

وقد خصص مشروع قانون العقوبات باباً خاصاً للجرائم الإلكترونية وهو الباب الثاني عشر، وقد وردت الجرائم الإلكترونية في مشروع قانون العقوبات دون أي تصنيف لها من حيث نوعها أو جسامتها أو تأثيرها:

- الدخول غير المشروع[5] ويشمل الدخول عمداً إلى موقع أو نظام معلوماتي[6]، وما ينتج عن ذلك من إلغاء أو حذف أو تدمير أو إعادة نشر بيانات أو معلومات.
- تزوير مستند من مستندات الحكومة، أو الهيئات، أو المؤسسات العامة، أو تزوير غيرها من المستندات إذا كان من شأن ذلك إحداث الضرر.
- إعاقة أو تعطيل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو البيانات، أو إدخال ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير البرامج أو حذفها أو اتلافها أو تعديلها أو البيانات أو المعلومات فيها.
- تعديل أو اتلاف الفحوص الطبية أو التشخيص الطبي أو العلاج الطبي أو الرعاية الطبية أو سهل لغيره فعل ذلك.
- التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات.
- تهديد شخص آخر أو ابتزازه لحمله على القيام بفعل أو الامتناع عنه.
- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع على هذا السند بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة لخداع المجني عليه.
- الوصول إلى أرقام أو بيانات بطاقة إئتمانية أو غيرها من البطاقات الإلكترونية باستخدام الشبكة المعلوماتية أو وسائل تقنية المعلومات.
- المساس بالآداب العامة عن طريق إنتاج أو تهيئة أو إعداد أو توزيع أو غيرها عن طريق الشبكة المعلوماتية أو وسائل تقنية المعلومات.
- التحريض على الدعارة أو إغواء ذكر أو أنثى لارتكاب العارة أو الفجور عن طريق الشبكة المعلوماتية أو وسائل تقنية المعلومات.
- الدخول لتغيير تصميم موقع إلكتروني أو إلغائه أو اتلافه أو تعديله أو شغل عنوانه.
- الإساءة أو سب إحدى المقدسات أو الشعائر المقررة للأديان السماوية، أو تجرأ بالعيب على الذات الإلهية أو الأنبياء والرسل.

---

[5] حسب مشروع قانون العقوبات الدخول غير المشروع هو: دخول شخص بطريقة متعمدة إلى حاسب آلي أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها.

[6] هو مجموعة من البيانات والتعليمات والأوامر القابلة للتنفيذ بوسائل تقنية المعلومات، ومعدة لإنجاز مهمة ما.

- الاعتداء على أي من المبادئ أو القيم الأسرية، أو نشر أخبار أو صور تتصل بحرمة الحياة الخاصة ولو كانت صحيحة، أو التشهير بالآخرين.
- الاتجار في الأشخاص سواء بإنشاء موقع أو نشر معلومات على الشبكة المعلوماتية.
- الترويج للمخدرات أو المؤثرات العقلية وما في حكمها، أو تسهيل التعامل فيها.
- تحويل الأموال غير المشروعة أو نقلها، أو تمويه المصدر غير المشروع لها، أو إخفائه، أو استخدام الأموال أو اكتسابها، أو حيازتها، مع العلم بأنها مستمدة من مصدر غير مشروع.
- الإخلال بالنظام العام والآداب العامة سواء بإنشاء موقع أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لأية مجموع تدعو لتسهيل برامج وأفكار أو ترويجها.
- دعم الجماعات الإرهابية سواء بإنشاء موقع أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها ...
- الحصول على بيانات أو معلومات حكومية سرية.
- انتهاك حقوق الملكية الفكرية سواء ما يتعلق بالأعمال الأدبية أو الفنية أو التصويرية.
- فك مفاتيح التشفير الإلكترونية، أو القيام بذلك بمقتضى الوظيفة.
- تحريض أو مساعدة شخص آخر على ارتكاب جريمة من الجرائم السابقة.
- الشروع في ارتكاب أي من الجرائم الإلكترونية السابقة الذكر.

كما جاء في مشروع قانون المعاملات الإلكترونية الجرائم التالية المتعلقة بالزوير:

- التزوير أو التلاعب في توقيع أو أداة[7] أو نظام توقيع إلكتروني للحكومه أو للهيئات أو للمؤسسات العامه سواء تم ذلك باصطناعه أوإتلافه أو تعييبه أو تعديله أو تحويره أو بأي طريقة أخرى تؤدي إلى تغيير الحقيقية في بياناته .
- إنشاء أو التواطؤ مع الغير لإنشاء بيانات توقيع أو أداة نظام توقيع إلكتروني للحكومه أو للهيئات أو للمؤسسات العامه.
- استعمال المستند المزور مع علم الشخص بالتزوير.
- استعمال عناصر تشفير شخصيه متعلقه بامضاء الغير.
- قيام الشخص بطريقه غير مشروعه بكشف مفاتيح لفك التشفير أو فك تشفير معلومات مودعه لديه.
- القيام عمدا بفك بيانات مشفره بأية طريقه في غير الاحوال المصرح بها قانونا.
- استعمل بصفه غير مشروعه أداة انشاء توقيع متعلقه بتوقيع شخص أخر.
- القيام عمدا بانشاء أو نشر شهاده أو زور بمعلومات الكترونيه غير صحيحه لغرض غير مشروع. عدم إخطار الهيئة بأي تغيير في البيانات التي حصل بناء عليها على الترخيص بتقديم خدمات تتعلق بالمعاملات الإلكترونية للجمهور.
- تقديم متعمدا بيانات غير صحيحة عن هويته إلى مزود خدمات المصادقة الإلكترونية بغرض طلب استصدار أو إلغاء أو إيقاف الشهادة.
- إصدار شهادات أو تقديم أي خدمات تتعلق بالتوقيع الالكتروني دون الحصول على ترخيص من الهيئة.

[7] عرف مشروع القانون أداة التوقيع هي برنامج يستعمل لإنشاء توقيع إلكتروني على معاملة.

- أضاف مشروع قانون المعاملات الإلكترونية إلى ما سبق: التوصل عن طريق الشبكة المعلوماتيه أو احدى وسائل تقنية المعلومات الى الاستيلاء لنفسه أولغيره على توقيع الكتروني أو بيانات انشاء توقيع الكتروني أو منظومة انشاء توقيع الكتروني أو وثيقه الكترونية، او اختراق أي منها أو اعتراضها أو تعطيلها عن أداء وظيفتها, وذلك بالاستعانة بطريقة احتياليه أو باتخاذ اسم كاذب أو انتحال صفه غير صحيحه متى كان ذلك من شأنه خداع المجني عليه.

وبالرغم من معالجة الأحكام القانونية للكثير من الجرائم الإلكترونية، وتشابهها مع ما ورد في كثير من قوانين الدول الأخرى، إلا أن هناك كثير من أنوا ع الجرائم الإلكترونية لم تتم الإشارة إليها في كل من مشروع المعاملات الإلكترونية أو مشروع قانون العقوبات، وقد وردت في كثير من قوانين الدول الأخرى، وأهمها:

- اعتبر القانون العماني جريمة إلكترونية استخدام تقنية المعلومات في المقامرة أو الترويج لبرامج أو أفكار أو أنشطة من شأنها ذلك.
- اعتبر القانون الأردني والسوداني جريمة إلكترونية الدخول قصداً دون تصريح أو بما يخالف أو يجاوز التصريح إلى موقع الكتروني أو نظام معلومات باي وسيلة كانت بهدف الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية السلامة العامة أو الاقتصاد الوطني.
- اعتبر كل من القانون الإماراتي والعماني الدخول بغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك. ويسري ذلك على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.
- اعتبر القانون العماني جريمة إلكترونية إنشاء موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار بالأسلحة والذخائر أو تسهيل التعامل فيها.
- اعتبر القانون العماني جريمة إلكترونية إنشاء موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار بالآثار والتحف الفنية في غر الأحوال المصرح بها قانوناً.
- اعتبر كل من القانون العماني والقطري جريمة إلكترونية تزوير بطاقة مالية أو استعملها أو قدمها للغير أو سهل الحصول عليها أو استخدم الشبكة المعلوماتية أو وسائل تقنية المعلومات في الوصول دون وجه حق إلى أرقام أو بيانات بطاقة مالية، أو قبل بطاقة مالية مزورة وهو يعلم بذلك. أو الاستيلاء على أموال الغير أو على ما تتيحه البطاقة من خدمات.
- جاء القانون القطري اكثر تفصيلاً فيما يتعلق بالفيروسات إذ اعتبر جريمة إلكترونية كل من سجل، أو زرع عمداً فيروساً على الأقراص، أو الإسطوانات الخاصة بحاسب آلي مملوك للغير، بقصد تدمير برامجه، أو بياناته المسجلة، أو المخزنة في داخله، أو استخدام الفيروس لبطء تشغيل نظام الحاسب الآلي عن معدله الطبيعي. أو إذا ترتب على استخدام الفيروس تدمير البرامج، أو البانيات المسجلة أو المخزنة في داخل الحاسب الآلي. وكل من غير في الحقيقة أو عدل في االمعلومات، أو البيانات، أو البرامج المخزنة في جهاز حاسب آلي مملوك للغير، أو محا بعضها عن طريق استخدام الفيروس، أو أي طريق آخر غير مشروع.
- أن يشمل القانون على الشروط والضمانات التي توفر الحماية الكافية لحقوق الإنسان والحريات الأساسية الأخرى، ولما جاء في العهد الدولي الخاص لسنة 1966 للأمم المتحدة الخاص بالحقوق المدنية والسياسية والدولية وحقوق الإنسان الأخرى. حسب ما جاء في اتفاقية بودابست.

- أكد القانون السويدي على أن تطبيق أحكام القانون إلى المدى الذي يتعارض مع الأحكام المتعلقة بحرية الصحافة وحرية التعبير. كما انه عند معالجة البيانات الشخصية فإنه يحظر الكشف عن الأصل العرقي أو الإثني، أو الآراء السياسية، أو المعتقدات الدينية أو الفلسفية، أو العضوية في أي نقابة. ويحظر أيضا الكشف عن المخاوف الصحية أو التمتع بحياة جنسية. كما يحظر نقل البيانات إلى بلد آخر إلا بضمان الحماية الكافية للبيانات الشخصية، وإيلاء اهمية خاصة إلى طبيعة البيانات، والغرض من المعالجة، ومدة المعالجة.
- أكدت اتفاقية بودابست على ضرورة اعتماد الصلاحيات الكافية لمكافحة مثل هذه الجرائم بشكل فعال، من خلال تسهيل على الكشف والتحقيق والملاحقة القضائية على الصعيدين المحلي والدولي وتوفير ترتيبات سريعة وموثوق بها التعاون الدولي. مع الأخذ بعين الاعتبار ضرورة احترام حقوق الإنسان الأساسية الواردة في الاتفاقيات الدولية، والحق في حرية التعبير، وحرية تلقي ونقل المعلومات والأفكار، والحق في حماية البيانات الشخصية.

3-5 العقوبات على الجرائم الإلكترونية

فرض مشروع قانون العقوبات عقوبة محدد لكل جريمة من الجرائم الإلكترونية سابقة الذكر، وهناك 11 مستوى من العقوبات التي تراوحت ما بين عقوبة الحبس، والحبس لمدة 10 سنوات والغرامة المالية التي تراوحت ما بين 1400 دولار[8] و28 ألف دولار. ويمكن إجمال هذه العقوبات فيما يلي:

1. الحبس لجريمة تعديل أو اتلاف الفحوص الطبية.
2. الحبس والغرامة للجرائم التالية:
   - الدخول غير المشروع.
   - تزوير مستندات غير المستندات الحكومية أو المؤسسات العامة.
   - استعمال السندات المزورة غير الحكومية.
   - إعاقة أو تعطيل الوصول إلى الخدمة.
   - التنصت أو اعتراض ما هو مرسل من الشبكة المعلومايتة.
   - الوصول إلى أرقام بيانات بطاقة إئتمانية.
   - المساس بالأداب العامة.
   - دخول لتغيير تصميم موقع أو إلغاؤه أو اتلافه.
   - سب إحدى المقدسات أو الشعائر المقررة في الأديان السماوية.
3. حبس مدة لا تزيد عن 6 أشهر وبغرمة لا تتجاوز 1400 دولار أو بإحدى هاتين العقوبتين، للجرئم التالية:
   - دخول أدى إلى حذف أو تغيير أو اتلاف معلومات.
   - استخدام بطافة إئتمانية للحصول على أموال شخص غيره.
   - انتهاك حقوق الملكية الفكرية.
4. حبس مدة لا تقل عن سنة وغرامة مالية لا تتجاوز 4200 دولار أو بإحدى العقوبتين، لجريمة الدخول غير المشروع بحكم تأدية الشخص لوظيفته.

[8] حولت العملات المستخدمة في القوانين ومشروع القانون إلى الدولار وفقاً لأسعار الصرف التالية: الريال العماني = 2.59 دولار، والدينار الأردني= 1.4 دولار، والدرهم الإماراتي= 0.27 دولار، والريال القطري= 0.27 دولار، والين الياباني=0.013 دولار، واليرو= 1.4 دولار.

5. حبس مدة لا تقل عن سنة وغرامة مالية لا تتجاوز 7000 دولار أو بإحدى العقوبتين، للجرائم التالية:
   - ✧ الاستيلاء على مال منقول.
   - ✧ استخدام بطاقة إئتمانية للاستيلاء على أموال الغير.
   - ✧ المساس بالآداب العامة للطفل.
   - ✧ الاعتداء على القيم الأسرية والتشهير بالآخرين.
   - ✧ فك التشفير لمحرر، أو استعمال كلمة المرور بمقتضى الوظيفة.
6. حبس مدة لا تزيد على سنة وغرامة مالية لا تتجاوز 1400 دولار لفك مفاتيح التشفير الإلكترونية.
7. الحبس لمدة لا تزيد على سنتين وبغرامة لا تتجاوز 7000 دولار أو بإحدى العقوبتين لجريمة التهديد أو ابتزاز شخص لحمله على القيام بفعل أو الامتناع عنه.
8. السجن المؤقت للجرائم التالية:
   - ✧ تزوير مستندات حكومية أو مؤسسات عامة.
   - ✧ الاتجار في الأشخاص.
   - ✧ الترويج للمخدرات.
   - ✧ الحصول على معلومات سرية حكومية.
   - ✧ تعطيل شبكة المعلومات أو إيقافها وغرمة لا تقل عن 14 ألف دولار.
9. السجن مدة لا تزيد على 5 سنوات، للجرائم التالية:
   - ✧ الإخلال بالنظام العام والآداب.
   - ✧ دعم الجماعات الإرهابية.
   - ✧ الاطلاع على معلومات حكومية سرية واتلافها وتدميرها أو نشرها.
10. السجن مدة لا تقل عن 5 سنوات والغرمة لا تتجاوز 7000 دولار لجريمة إغواء شخص لارتكاب الدعارة أو الفجور ولو لم تقع الجريمة إذا كان المجني عليه طفلاً.
11. السجن مدة لا تزيد على 7 سنوات وبعرامة لا تتجاوز 28 ألف دولار لتحويل الأموال غير المشروعة.
12. السجن 10 سنوات إذا التهديد والابتزاز لشخص لارتكاب جناية أو أمور خادشة للشرف.
13. السجن والغرامة لتحريض ذكر أو أنثى أو إغوائه لارتكاب الدعارة أو الفجور، أو ساعده على ذلك.
14. فرض مشروع القانون نصف العقوبة في حالة الشروع في الجريمة الإلكترونية.
15. فرض مشروع القانون ثلثي العقوبة في حالة التحريض أو المساعدة أو الاتفاق على ارتكاب الجريمة الإلكترونية.

أما العقوبات التي وردت في مشروع قانون المعاملات الإلكترونية فهي:

- ✧ السجن المؤقت لاقتراف تزوير أو تلاعب في نظام توقيع إلكتروني للحكومه أو للهيئات أو للمؤسسات العامه. أو التواطؤ مع الغير لإنشاء بيانات توقيع أو أداة نظام توقيع إلكتروني.
- ✧ الحبس وبغرامه لا تتجاوز 7000 دولار للاطلاع من قبل شخص صاحب صلاحيات على معلومات في سجلات أو مستندات أو مراسلات الكترونيه، أو كشف مفاتيح لفك التشفير، أو الاستيلاء لنفسه أولغيره على توقيع الكتروني.

- ✧ الحبس وبغرامه لا تقل عن 4200 دولار أو باحدى هاتين العقوبتين كل من استعمل بصفة غير مشروعه عناصر تشفير شخصيه متعلقه بامضاء غيره، أو نشر شهاده أو زور بمعلومات الكترونيه، أو شهادات أو تقديم أي خدمات تتعلق بالتوقيع الالكتروني، أو منع عمدا أحد رجال الضبطيه القضائيه او المأذون بالاستعانه بهم في اجراء التفتيش.
- ✧ الحبس لمدة لا تزيد عن ستة اشهر وبغرامة لا تزيد عن 1400 دولار كل من قدم متعمدا بيانات غير صحيحة عن هويته إلى مزود خدمات المصادقة الإلكترونية بغرض طلب استصدار إو إلغاء أو إيقاف الشهادة.
- ✧ مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة، ويحكم باغلاق المحل أو الموقع الذي يرتكب فيه أي من هذه الجرائم اذا كانت الجريمة قد ارتكبت بعلم مالكها، وذلك إغلاقا كليا أو للمدة التي تقدرها المحكمة.
- ✧ مع عدم الإخلال بأي عقوبة أشد ينص عليها أي قانون آخر يعاقب كل من ارتكب فعلا يشكل جريمة بموجب التشريعات النافذة، باستخدام وسيلة الكترونيه بالحبس لمدة لاتزيد عن سنة وبغرامة لاتزيد عن 4200 دولار أو ما يعادلها بالعملة المتداولة قانونا أو بإحدى هاتين العقوبتين ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في قانون المعاملات الإلكترونية.
- ✧ يحق للهيئه ودون الحاجه الى اذن قضائي اغلاق أي محل أو شركه تقوم بتقديم خدمات المصادقه الالكترونية دون الحصول على ترخيص بذلك .
- ✧ للهيئه اذا خالف المرخص له شروط الترخيص أو خالف أحكام هذا القانون أن تلغي الترخيص كما يكون لها أن توقف سريانه حتى ازالة أسباب المخالفه.
- ✧ منح القانون عدد من موظفي الهيئة العامة للمصادقة الإلكترونية صفة الضبطيه القضائيه[9] وعلى السلطات المدنيه أو أجهزة الامن أن تقدم لهم كل مساعده ممكنه للقيام بمهامهم.

وفيما يلي بعض الملاحظات على هذه العقوبات:

أولا– وفقاً لمشروع لقانون العقوبات فإن فإن الحد الأدنى لعقوبة الحبس 24 ساعة. وقد يكون السجن مؤقتاً أي لا تقل مدته عن 3 سنوات ولا تزيد على 15 سنة. أو السجن المؤبد وهو لمدة 20 سنة. أو السجن مدى الحياة.

وبناء على هذا التعريف فإن ما ورد في العقوبة المفروضة على عدة جرائم إلكترونية من عقوبة الحبس دون أن تحدد مدته يعد خللاً في مشروع القانون وقد ورد فرض هذه العقوبة 10 مرات دون تحديد مدة الحبس. ولذلك لا بد من تعديل مشروع القانون بتحديد المدة الزمنية للعقوبة، إذ أن النص القانوني يجدر ألا يحتوي على أحكام غامضة أو مطلقة.

ثانياً– يلاحظ من خلال الاطلاع على هذه العقوبات، أن العقوبة المفروضة على بعض الجرائم الإلكترونية لا تتناسب مع الأثر المترتب على الجريمة الإلكترونية؛ حيث أنه من المفروض أن تكون العقوبة أشد كلما كان أثر الجريمة أكبر؛ مما يستدعي إعادة النظر في هذه العقوبات وتعديلها حتى تتناسب مع حجم الجريمة الإلكترونية، ومن الأمثلة على ذلك:

[9] يعني ذلك أن كل ما يصدر عن موظفي الهيئة في مجال عملهم يعتبر كأنه يصدر عن شرطي.

- الحبس لمدة لا تقل عن 6 أشهر وبغرامة لا تتجاوز 1400 دولار لكشف مفاتيح لفك التشفير وتتضاعف الغرامة إلى 7000 دولار إذا استعملها. والحبس وبغرامه لا تقل عن 4200 دولار لكل من استعمل بصفة غير مشروعه عناصر تشفير شخصيه متعلقه بامضاء غيره. وهنا يجدر أن تكون عقوبة الحبس أشد على جريمة استعمال عناصر تشفير شخصية متعلقة بالغير، أكثر منها على جريمة فك عناصر التشفير.
- ما يتعلق بالعقوبات التي وردت في البند 8 أعلاه يلاحظ أن المشروع قد فرض الغرامة المالية في حالة تعطيل الشبكة المعلوماتية فقط، في حين يجب فرض غرامة مالية على الجرائم الأخرى في هذا البند خاصة وأنها أدت إلى تكسب مالي كبير غير مشروع كالاتجار في المخدرات والاتجار في الأشخاص.
- يلاحظ اقتصار العقوبات على تزوير السندات الحكومية، أو الاطلاع على معلومات حكومية سرية. ولكن يجدر بالقانون أن يراعي حقوق الأطراف الأخرى وخاصة القطاع الخاص، وأن تشمل الجريمة الاطلاع على معلومات تتعلق بشركات أو مؤسسات القطاع الخاص أو تزوير السندات المتعلقة بها.

ويلاحظ أن مشروع القانون يتشابه إلى حد كبير في مسألة العقوبات، ولكن يمكن الاستفادة من قوانين الدول الأخرى من خلال الملاحظات التالية:

- تشدد كل القانون العماني واتفاقية بودابست في مضاغفة الحد الأعلى لعقوبة الغرامة المقررة قانوناً للجريمة إذا كان الشخص اعتبارياً وكانت الجريمة قد ارتكبت باسمه أو لحسابه من قبل رئيس أو أحد أعضاء مجلس إدارته أو مديره أو مسؤول آخر يتصرف بتلك الصفة أو بموافقته أو بتستر أو بإهمال جسيم منه، ودون الإخلال بالمسؤولية الجزائية للأشخاص الطبيعيين. في حين لم يرد ذكر ذلك في مشروع قانون العقوبات.
- القانون الأردني أنه وضع حداً أدنى وحداً أعلى لعقوبة السجن تراوحت ما بين أسبوع و6 أشهر كما وضع حداً أدنى وحداً أعلى لعقوبة الغرامة المالية تراحت ما بين 280 إلى 7000 دولار. إضافة إلى القانون يطبق العقوبتين معاً وليس أحدهما كما جاء في مشروع القانون. وكذلك القانون العماني وضع حداً أدنى وحداً أعلى لعقوبة السجن تراوحت ما بين الحبس شهر واحد و3 سنوات، كما وضع حداً أدنى وحداً أعلى لعقوبة الغرامة الماية تراحت ما بين 259 دولار 7770 دولار لمعظم الجرائم الإلكترونية. في حين لم يرد مثل ذلك في 10 حالات كما سبق ذكره.
- القانون السوداني لم يحدد قيمة الغرامة المالية، والعقوبة قد تكون الحبس أو الغرامة المالية أو كلتيهما. ولكن تشدد أكثر في فرض عقوبة الحبس إذ تراوحت مدة الحبس من سنتين إلى 7 سنوات في غالبية الجرائم الإلكترونية.
- تشددت قوانين الدول الأخرى كثيراً كالقانون السوداني والعماني والإماراتي في العقوبات المفروضة على الجرائم الإلكترونية الكبيرة التي قد تمس أمن الدولة أو الأمن الاقتصادي أو غسيل الأموال أو الاتجار بالبشر أو ترويج المخدرات، فقد تصل فيها العقوبة السجن 10 سنوات أو 20 سنة أو السجن المؤبد. مقارنة مع سجن 7 سنوات في مشروع قانون العقوبات.
- يلاحظ أن القانون الإماراتي قد تشدد بشكل أكثر في فرض عقوبة السجن المؤقت لكل من عدل أو أتلف الفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية. مقارنة مع عقوبة الحبس فقط كما ورد في مشروع قانون العقوبات.

4-5 قضايا أخرى لم ترد في الأحكام المتعلقة بالجرائم الإلكترونية

عملت كثير من الدول على اتخاذ إجراءات أخرى للحد من الجرائم الإلكترونية، وقد قام بعض هذه الدول بالنص على ذلك في القوانين ذات العلاقة، ومن هذه الإجراءات:

- ✧ نص القانون السوداني على إنشاء محكمة خاصة للجرائم الإلكترونية، ويجوز لرئيس القضاء إصدار قواعد خاصة لتحديد الإجراءات التي تتبع في هذه المحاكم، كما نص على إنشاء نيابة متخصصة في جرائم المعلوماتية، وكذلك إنشاء شرطة متخصصة لجرائم المعلوماتية.
- ✧ أكدت اتفاقية بودابست على ضرورة التعاون بين الدول والقطاع الخاص في مكافحة الجرائم الإلكترونية والحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات. كما أن النظام الفعال لمكافحة الجريمة الحاسوبية يتطلب زيادة سريعة وجيدة الأداء التعاون الدولي في المسائل الجنائية.

وافقت دول الاتحاد الأوروبي في حزيران 2011 نهائيا بانتظار موافقة البرلمان الأوروبي على فرض عقوبات أكثر صرامة ضد مرتكبي الجرائم الالكترونية ومنفذي الهجمات على أنظمة الكمبيوتر، وبموجب هذه العقوبات فإن الذين يقومون بأعمال الاختراق او القرصنة الكترونية يواجهون حكما بالسجن لمدة 5 سنوات على الأقل في حالة إدانتهم بالتسبب في أضرار جسيمة لأنظمة تكنولوجيا المعلومات. وسيفرض عقوبات أكثر صرامة على مرتكبي الهجمات من خلال ما يعرف ببرنامج بوت نت الذي يربط أجهزة الكمبيوتر بنظام متطفل لإرسال رسائل البريد الالكتروني غير المرغوب فيها بهدف انتحال الهوية. كما ان اعتراض البيانات بطرق غير مشروعة أصبح جريمة جنائية في الاتحاد الأوروبي. وقررت دول الاتحاد أيضا تعزيز تعاونهما القضائي والأمني عن طريق إنشاء وحدة لجرائم الالكترونية ستكون على صلة بجهاز الشرطة الاتحادي الأوروبي (يوروبول). وتبذل الحكومات في جميع أنحاء العالم جهودا حثيثة لبلورة استراتيجيات الأمن الالكتروني بسبب مخاوف متزايدة من أنشطة القراصنة واحتمالات تسجيل نوع جدي من الحروب الرقمية على مستوى المؤسسات او حتى الدول (www.raj3elsada.com).

- ✧ تم في الإمارات إنشاء وحدات خاصة للبحث الجنائي الإلكتروني والمختبر الجنائي الإلكتروني، إضافة إلى تسيير شرطة الإنترنت التي تعمل على ضبط أي مخالفات على الشبكة المعلوماتية.
- ✧ تم في نهاية العام 2009 افتتاح مركز مكافحة الجرائم الالكترونية التابع لإدارة البحث الجنائي في قطر بالتعاون مع جمهورية كوريا الجنوبية والذي يعد من المراكز المعنية بمكافحة الجرائم الالكترونية على مستوى المنطقة، إذ يمتاز بتطبيقه واستخدامه لأحدث الأجهزة في مكافحة هذا النوع من الجرائم (www.qatarshares.com).
- ✧ أعلن في لندن في بداية تموز/2011 عن تأسيس التحالف الدولي لمكافحة الجرائم الالكترونية على مستوى العالم. بتمويل من الاتحاد الأوروبي وحكومات بعض الدول. ويضم التحالف حكومات دول وكبرى وكالات تنفيذ القانون بما فيها هيئة الشرطة الأوروبية "اليوربول". كما انضمت للتحالف شركتا مكافي وترينذ مايكرو(McAfee& Trend Micro) للأمن الالكتروني. والهدف من التحالف الجديد هو تحسين قدرة تنفيذ القانون الدولي والمساعدة على حماية الشركات وعملائها ضد هذا التهديد (www.bbc.co.uk).

6- النتائج والتوصيات

يعرض هذا الجزء من الدراسة أهم النتائج التي توصل إليها البحث، وأهم التوصيات التي من شأنها أن تعمل على تطوير مشروع قانون للجرائم الإلكترونية يتلائم مع التطورات التكنولوجية في مجال تكنولوجيا الاتصال والمعلوماتية ويشمل على عقوبات للجرائم الإلكترونية المختلفة، عله يساعد على مكافحة هذه الجرائم بشكل فعال، والحد من وقوعها.

6-1 النتائج

أهم النتائج التي توصلت إليها الدراسة هي:

1. إن الجرائم الإلكترونية ظاهرة موجودة في الأراضي الفلسطينية، وأن انتشارها بدأ بالتزايد منذ بضع سنوات. ولكن نظراً لعدم وجود قانون أو منظومة قوانين حديثة لمكافحتها فإنه لا يتوفر بيانات رسمية موثوقة حول مستويات انتشار وأنواع ومخاطر هذه الجرائم. إذ يتم تصنيفها تحت بند الجرائم الأخرى التي يوجد لها نصوص قانونية مباشرة.
2. يتأثر انتشار هذه الجرائم بانتشار استخدام الإنترنت في الأراضي الفلسطينية بشكل طردي، وبارتفاع معدلات البطالة، وعدم وجود القانون الملائم الذي يعاقب على الجريمة الإلكترونية، والقصور في برامج التوعية والتحذير من خطورة هذه الجرائم. إضافة إلى عدم وجود سيادة فلسطينية على مجالات الترددات الكهروميغناطيسية، وتدخل شبكات الاتصالات الفلسطينية بالشبكة الإسرائيلية.
3. اتخذت السلطة الفلسطينية العديد من الإجراءات للحد من انتشار الجرائم الإلكترونية والعمل على مكافحتها، وأهم هذه الإجراءات: إنشاء وحدة مكافحة الجرائم الإلكترونية في القيادة العامة للشرطة الفلسطينية، وتخصيص فصل خاص في مشروع قانون العقوبات لجرائم الحاسوب؛ حيث ترد نصوص حول أنواع الجرائم الإلكترونية، وفرض عقوبة على كل واحدة منها. وكذلك ذكر العقوبات المتعلقة بكل جريمة إلكترونية فيما يتعلق بالمعاملات الإلكترونية في مشروع قانون المعاملات الإلكترونية.
4. تنسجم النصوص المتعلقة بالجرائم الإلكترونية مع ما ورد في القانون الأساسي الذي كفل الحرية الشخصية كرامة الفرد. كما يأتي هذا المشروع مكملاً لبعض القوانين الأخرى مثل القرار بقانون المصارف رقم 9 لسنة 2010، وقانون الأوراق المالية رقم 12 لسنة 2004، اللذان نصت أحكامهما على استخدام الوسائل التكنولوجية في عملياتها، أو لطرق الإثبات فيها. ولكن لم يحددا عقوبة لارتكاب جريمة إلكترونية. وإلى قانون الاتصالات السلكية واللاسلكية رقم 3 لسنة 1996، وقانون العقوبات اللذان لم يتطرقا إلى استخدام الإنترنت أو ما يتعلق بالجرائم الإلكترونية.
5. جاءت معظم النصوص المتعلقة بالجرائم الإلكترونية في مشروع قانون العقوبات الفلسطيني، وجاء جزء منها وهو المتعلق بتزوير التوقيع الإلكتروني وما شابه من الجرائم الإلكترونية في مشروع قانون المعاملات الإلكترونية. وهذا قد يسبب في تأجيل سن التشريع المتعلق بالجرائم الإلكترونية بسبب ما يتعلق بمشروع قانون العقوبات من بعض العوامل السياسية (تعطل عمل المجلس التشريعي... الخ) التي تؤجل إصداره.

6. بالرغم من معالجة الأحكام القانونية في مشروعي قانوني المعاملات الإلكترونية والعقوبات للكثير من الجرائم الإلكترونية، وبصورة مشابهة لما ورد في كثير من قوانين الدول الأخرى، إلا أن هناك كثير من أنواع الجرائم الإلكترونية التي وردت في كثير من قوانين الدول الأخرى لم تجر الإشارة إليها في كل من مشروع المعاملات الإلكترونية أو مشروع قانون العقوبات.
7. إن عقوبة الحبس التي وردت ضمن العقوبات المفروضة على الجرائم الإلكترونية دون أن تحديد مدته يعد خللاً في مشروع القانون. فقد ورد فرض هذه العقوبة 10 مرات دون تحديد مدة الحبس، مما يضعف من وظيفة القانون لردع الجريمة الالكترونية، ويخلق غموضا لا مبرر له ويجعل من تحقيق العدالة أمرا صعبا.
8. لا تتناسب العقوبات أحياناً مع الأثر المترتب على الجريمة الإلكترونية وقد ورد العديد من الأمثلة على ذلك في متن الدراسة.
9. لم يرد في النصوص المتلعقة بالجرائم الإلكترونية بعض الإجراءات الأخرى للحد من الجرائم الإلكترونية، مثل إنشاء محكمة خاصة للجرائم الإلكترونية، وإنشاء نيابة متخصصة في جرائم المعلوماتية، إنشاء شرطة متخصصة لجرائم المعلوماتية.

6-2 التوصيات

على ضوء النتائج التي توصلت إليها الدراسة، فإنها تقترح التوصيات التالية:

1. العمل على صياغة مشروع قانون خاص بالجرائم الإلكترونية أسوة بمعظم الدول الأخرى، وأن يشير مشروع القانون إلى استخدم الحاسوب وجميع وسائل تقنية ونقل المعلومات، وليس الحاسوب فقط لارتكاب هذه الجرائم.
2. أن ينص على أنواع أخرى من الجرائم الإلكترونية التي لم ترد في أي من مشروعي قانوني العقوبات والمعاملات الإلكترونية، وأهمها استخدام الشبكة المعلوماتية أو تقنية المعلومات للقيام بأي مما يلي:

- ✧ استخدام تقنية المعلومات في المقامرة أو الترويج لبرامج أو أفكار أو أنشطة من شأنها ذلك.
- ✧ الاطلاع على بيانات أو معلومات غير متاحة للجمهور تمس الأمن الوطني أو العلاقات الخارجية السلامة العامة أو الاقتصاد الوطني.
- ✧ الدخول بغير وجه حق موقعاً أو نظاماً مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات خاصة بالمنشآت المالية والتجارية والاقتصادية.
- ✧ إنشاء موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار بالأسلحة والذخائر أو تسهيل التعامل فيها.
- ✧ إنشاء موقع إلكتروني أو نشر معلومات على الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الاتجار بالآثار والتحف الفنية في غر الأحوال المصرح بها قانوناً.
- ✧ أن يشمل القانون على الشروط والضمانات التي توفر الحماية الكافية لحقوق الإنسان والحريات الأساسية الأخرى، ولما جاء في العهد الدولي الخاص لسنة 1966 للأمم المتحدة الخاص بالحقوق المدنية والسياسية والدولية وحقوق الإنسان الأخرى.
- ✧ أن تطبيق أحكام القانون إلى المدى الذي يتعارض مع الأحكام المتعلقة بحرية الصحافة وحرية التعبير.

- ضرورة اعتماد الصلاحيات الكافية لمكافحة مثل هذه الجرائم بشكل فعال، من خلال تسهيل الكشف والتحقيق والملاحقة القضائية على الصعيدين المحلي والدولي وتوفير ترتيبات سريعة وموثوق بها التعاون الدولي. مع الأخذ بعين الاعتبار ضرورة احترام حقوق الإنسان الأساسية الواردة في الاتفاقيات الدولية، والحق في حرية التعبير، وحرية تلقي ونقل المعلومات والأفكار، والحق في حماية البيانات الشخصية.

3. هناك بعض الأمور الهامة التي يجب مراعاتها فيما يتعلق بالعقوبات:
   - أن يعمل مشروع القانون بتحديد المدة الزمنية لعقوبة السجن أو أن يضع حداً أدنى وحداً أعلى لمدة الحبس، وأن يضع حداً أدنى وحداً أعلى لقيمة الغرامة المالية كذلك.
   - أن يراعي المشروع ملائمة العقوبة للجريمة بحيث تكون العقوبة أشد كلما كانت الجريمة أكبر أو أثرها سلبياً أكثر.
   - أن يراعي مشروع القانون بعض الأمور الأخرى المتعلقة بالعقوبات، مثل:
     - مضاغفة الحد الأعلى لعقوبة الغرامة المقررة قانوناً للجريمة إذا كان الشخص اعتبارياً.
     - التشدد في العقوبات المفروضة على الجرائم الإلكترونية الكبيرة التي قد تمس أمن الدولة أو الأمن الاقتصادي أو غسيل الأموال أو الاتجار بالبشر أو ترويج المخدرات.
4. أن يشير المشروع إلى بعض القضايا الهامة الأخرى مثل:
   - أن تأخذ قضايا الجرائم الإلكترونية صفة الاستعجال.
   - انتداب قاض متخصص للبت في الجرائم الإلكترونية.
   - ضرورة التعاون بين الدول والقطاع الخاص في مكافحة الجرائم الإلكترونية والحاجة لحماية المصالح المشروعة في استخدام وتطوير تكنولوجيا المعلومات.
   - التعاون الدولي لمكافحة الجريمة الحاسوبية.
5. بالرغم من أن أهمية وضرورة سن قانون يعاقب على ارتكاب الجرائم الإلكترونية، إلا أن هناك ضرورة للقيام بالتوعية بخطورتها وتأثيرها على المجتمع باستخدام مختلف الوسائل، ومنها على سبيل المثال:
   - يمكن الإشارة إليها في المناهج المدرسية وفي مساقات الجامعات، مثل إدخال مادة أخلاقيات الانترنت ضمن المناهج الدراسة.
   - إصدار نشرات توعية للتعريف بها وبخطورتها.
   - عقد ورش عمل مختلفة ولفئات مختلفة من المجتمع تتناول الحديث عن هذه الجرائم.
   - تصميم برامج في الإذاعة والتلفزيون تتناول ما يتعلق بهذه الجرائم، ونشر بعض القصص بالرموز أو بأسماء وأماكن وهمية.
6. الاستعانة ببرامج أمن قوية ضد الفيروسات أو اختراقات أنظمة الحاسوب.
7. نظراً لتمتع مرتكبي الجرائم الإلكترونية بقدرات خاصة ومميزة فإنه يمكن الاستفادة من خبراتهم في تعزيز الحماية الإلكترونية للمؤسسات المختلفة.
8. العمل على عقد دورات تدريبية في كافة الجوانب المتعلقة بالجرائم الإلكترونية للعاملين في الجهات ذات العلاقة مثل أفراد الشرطة، والنيابة العامة والقضاة.

المراجـــــع

الألفي، محمد محمد صالح، 2011. أنماط جرائم الإنترنت. www.eastlaws.com

الجهاز المركزي للإحصاء الفلسطيني، 2011. المؤتمر الصحفي حول النتائج الرئيسية. المسح الأسري لتكنولوجيا المعلومات والاتصالات، 2011. رام الله- فلسطين.

الجهاز المركزي للإحصاء الفلسطيني، 2011. مسح القوى العاملة الفلسطينية: التقرير السنوي: 2010. رام الله ــ فلسطين.

جريدة القدس، 2011. 2011/9/29 صفحة 32.

جريدة القدس، 2011. 2011/7/28 صفحة 13.

السلطة الوطنية الفلسطينية. القانون الأساسي المعدل لسنة 2003.

السلطة الوطنية الفلسطينية. قانون رقم 3 لسنة 1996 بشأن الاتصالات السلكية واللاسلكية.

السلطة الوطنية الفلسطينية. قانون العقوبات رقم 16 لسنة 1960.

السلطة الوطنية الفلسطينية. قرار بقانون رقم 9 لسنة 2010 بشأن المصارف.

السلطة الوطنية الفلسطينية. قرار بقانون رقم (9) لسنة 2007 بشأن مكافحة غسل الأموال.

السلطة الوطنية الفلسطينية. قرار بقانون رقم (15) لسنة 2009 بشأن الهيئة الفلسطينية لتنظيم قطاع الاتصالات.

السلطة الوطنية الفلسطينية. قانون الأوراق المالية رقم 12 لسنة 2004.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم (3) لسنة 2004 بشأن منع بيع وتسويق خدمات الاتصالات وتقنية المعلومات والبريد السريع.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 34 لسنة 2004 بشأن إنشاء الشبكة الحكومية المستقلة للاتصالات.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 35 لسنة 2004 بشأن النفاذ إلى الشبكة العالمية (الإنترنت) والبريد الإلكتروني عبر مركز الحاسوب الحكومي.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 65 لسنة 2005 صدر بتاريخ 2005/5/10 بالمصادقة على اعتماد مبادرة فلسطين الإلكترونية.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 74 لسنة 2005 بشأن الاستراتيجية الوطنية للاتصالات وتكنولوجيا المعلومات.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 269 لسنة 2005 بالمصادقة على السياسات العامة لاستخدام الحاسوب وشبكة الإنترنت في المؤسسات العامة.

السلطة الوطنية الفلسطينية. قرار مجلس الوزراء رقم 276 لسنة 2005 بشأن تفعيل مركز الحاسوب الحكومي.

سمارة، مصطفى (2008). الجريمة الإلكترونية. أمن المعلومات، العدد (29)، شهر تموز 2008.

عبد الكريم، نصر والشعيبي، عزمي، (2008). التجربة الفلسطينية في مكافحة غسل الأموال. الائتلاف من أجل النزاهة والمساءلة (أمان). رام الله-فلسطين.

قانون جرائم أنظمة المعلومات قانون مؤقت لسنة 2010. الأردن.

القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات. الإمارات.

قانون جرائم المعلوماتية لسنة 2007. السودان.

مرسوم سلطاني رقم 2011/12 بإصدار قانون مكافحة جرائم تقنية المعلومات. عمان.

قانون العقوبات القطري رقم 11 لسنة 2004 فصل جرائم الحاسب الآلي المواد (370-387). قطر.

Councel of Europe, 2001. Convention on Cybercrime. Budapest.
Sweden, 1998.Personal Data Ordinance Act 204:1998.
Japan, 2003. The computer Misuse and Cybercrime Act No.22 of 2003.
www.infomag.news.sy
www.bbc.co.uk
www.emaratalyoum.com
www.moheet.com
www.bbc.co.uk
www. omarsalloum.7olm.org
www.raj3elsada.com
www.qatarshares.com
www.rosaonline.net