# تصنيف الجرائم الإلكترونية وفقاً لطبيعة الحق المعتدى عليه دراسة مقارنة بين التشريع الفلسطيني والإماراتي

**محمد بدوسي**

جامعة الاستقلال، فلسطين

**ma_badousi@pass.ps**

## الملخص

يتناول هذا البحث موضوع تصنيف وتنظيم الجرائم الإلكترونية، وأهميته في القانون الجنائي، مع التركيز على خصوصية وأهمية الحق المعتدى عليه كمعيار لهذا التصنيف في جميع مراحل المعالجة القانونية لمكافحة ظاهرة الإجرام الإلكتروني. كما تطرقنا في هذا البحث إلى منهج المشرعَيْنِ الفلسطيني والإماراتي في تصنيف وتنظيم الجرائم الإلكترونية، وذلك بموجب أحكام القرار بقانون رقم (10) لسنة 2018، وذلك بشأن الجرائم الإلكترونية، وجرائم الاتصالات وتكنولوجيا المعلومات، والمرسوم بقانون اتحادي رقم (34) لسنة 2021، وذلك بشأن مكافحة الشائعات والجرائم الإلكترونية. وفي نهاية الدراسة توصل الباحث إلى مجموعة من النتائج والتوصيات. وكان من بين أهم تلك النتائج التي توصل إليها الباحث أن تصنيف الجرائم الإلكترونية بالاستناد إلى معيار طبيعة الحق المعتدى عليه يشكل مسألة حيوية في مواجهة هذه الجرائم، إضافة إلى عدم اتباع المشرع الفلسطيني منهجاً معيناً لتصنيف الجرائم الإلكترونية والفصل بين أحكامها الموضوعية والإجرائية، وذلك على غرار ما فعل المشرع الإماراتي، الذي نظّم وصنف هذه الجرائم وفق منهج واضح، وكان من أهم التوصيات التي قدمها الباحث حثّ المشرع الفلسطيني القيام بإجراء بعض التعديلات على قانون الجرائم الإلكترونية، وتصنيف هذه الجرائم بناءً على معيار طبيعة الحق المعتدى عليه، وكذلك الفصل بين الأحكام الموضوعية والإجرائية في هذا القانون، والقيام بتعديل نصوص المواد (21،28، 48) من هذا القانون

**الكلمات المفتاحية:** التّقنيات الحديثة؛ الجرائم الإلكترونية؛ تصنيف الجرائم الإلكترونية؛ طبيعة الحق المعتدى عليه؛ معايير تصنيف الجرائم الإلكترونية

# CLASSIFICATION OF ELECTRONIC CRIMES ACCORDING TO THE NATURE OF THE RIGHT ASSAULTED

## (A COMPARATIVE STUDY BETWEEN THE PALESTINIAN AND EMIRATI LEGISLATIONS)

**Mohammad Badousi**

Alistiqlal University, Palestine

**ma_badousi@pass.ps**

## Abstract:

This research investigates the issue of the different classifications of electronic crimes, and the importance of classifying them in the criminal law, with a focus on the specificity and the importance of the right assaulted in classifying them, as well as the importance of classifying them according to this criterion at all stages of the legal process to Combatting phenomenon of electronic crime. In this study we also investigates, the approach of Palestinian and Emirati legislators in classifying and regulating the provisions electronic crimes and Communications Crimes & information technology, pursuant to Decree-Law No. 10 of 2018, and Federal Law Decree-Law No. 34 of 2021 on combating phenomenon of electronic crime. At the end of the study, the researcher reached a set of conclusions and recommendations, One of the most important of conclusions is that The classification of electronic crimes based on the criterion of the right assaulted constitutes a vital issue in confronting these crimes, just as the Palestinian legislator did not follow a specific approach in his classification of electronic crimes and their substantive and procedural provisions, as the UAE legislator did in organizing and classifying crimes according to a clear approach. One of the most important recommendations is the necessity of the legislator the need for the Palestinian legislator to make amendments to the electronic crimes Law, classify these crimes, and separate the substantive and procedural provisions within this law, as well as amend the texts of Articles (21, 28, 48) of this law.

**Keywords**: modern technologies; electronic crimes; classification of electronic crimes; the nature of right assaulted; criteria for classification of electronic crimes.

**Received: 01/11/2023** **Revised: 02/12/2023** **Accepted: 11/12/2023**

## المقدمة:

أدى التطور الذي حصل في مجال التكنولوجيا الحديثة إلى نمو سريع في ارتفاع نسبة المستخدمين لمختلف الوسائل التقنية التي نتجت عن هذا التطور، فأصبحت هذه الوسائل من أكثر الوسائل التي يعتمد عليها لتبادل المعلومات، الأمر الذي ساهم بظهور علاقات مختلفة تعتمد في وجودها وبنيتها الأساسية على هذه التقنيات

ولكن وعلى النقيض من الاستخدامات الإيجابية الكثيرة لهذه التقنيات، والتي نذكر منها على سبيل المثال لا الحصر، المجال الأمني والصناعي والاجتماعي والسياسي والاقتصادي والصحي وغيرها من الخدمات الحكومية، ظهر هناك جانب آخر سلبي تمثل في استغلالها لأغراض إجرامية في مختلف المجالات التي تستخدم بها هذه التقنيات في حياة الإنسان والمجتمع، هذا بدوره أدى إلى تنوع الجرائم التي تكون وسائلها أو موضوع الاعتداء فيها التكنولوجيا الحديثة

فجميع المؤشرات الحالية تشير إلى أن الاستغلال السيء لهذه التقنيات في ارتكاب الجرائم التي تقع في الوقت الحاضر، قد لا يتوقف عند هذا الحد؛ فالتطور التكنولوجي الذي أسهم في ظهورها وانتشارها لم يقف عند هذه المرحلة، وإنما هناك قابلية لاستمراره لاسيما في مجال استخدام تقنية الذكاء الاصطناعي،الأمر الذي قد يترتب عليه ظهور أنواع جديدة من الجرائم في المستقبل

(The Global Risks Report 2023 18th Edition Insight Report.p42)

ومن هنا، جاءت فكرة هذا البحث لتسليط الضوء على مسألة تنظيم و تصنيف هذه الجرائم في قانون الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني، وقانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي، وتسليط الضوء كذلك على ضرورة العمل على وضع تصنيف واضح ودقيق لهذه الجرائم في إطار التشريع الخاص بمكافحتها في النظام القانوني الفلسطيني، وبيان أهمية الاستناد إلى معيار طبيعة الحق المعتدى في تصنيفها، بالإضافة إلى بيان أهمية هذا التصنيف على صعيد العمل التشريعي والقضائي والفقهي؛ لاسيما في مجال تطوير التشريعات الخاصة بمكافحتها، وتحديد العقوبات التي قد تفرض على مرتكبيها بناء على أهمية الحق المعتدى عليه، ودور هذا التصنيف في عملية التكييف القانوني الصحيح لهذه الجرائم وإثباتها ومعاقبة مرتكبيها

## أهمية البحث:

يمثل البحث في هذا الموضوع أهمية كبيرة ترتبط بالتطور المستمر في مجال اعتماد الإنسان على وسائل التكنولوجيا الحديثة في مختلف مجالات حياته، وما صاحبه من استغلال سيء لهذه التقنيات، والذي تمثل في ظهور أنواع جديدة من الجرائم وارتكاب جرائم تقليدية بوسائل تكنولوجية حديثة، الأمر الذي يتطلب ضرورة العمل المستمر لتطوير الوعاء التشريعي الجنائي بشقه الموضوعي؛ لكي يستوعب الجرائم كافة، التي قد تظهر أو الجرائم التي قد تتطور وسائل ارتكابها بالتزامن مع تطور وسائل الاتصال والتواصل المختلفة، وعليه يأتي هذا البحث لمعالجة مسألة تصنيف الجرائم التي تقع أو التي قد تقع مستقبلا في هذا المجال لكي يسهل تنظيمها من الناحية القانونية. كما تأتي أهمية هذا البحث من خلال إجراء المقارنة بين التشريعين الفلسطيني والإماراتي باعتباره واحد من التشريعات الهامة على صعيد مكافحة الجرائم الإلكترونية؛ وذلك بهدف الاستفادة من هذه التجربة في تنظيم أحكام الجرائم الإلكترونية في التشريع الفلسطيني

## إشكالية البحث:

بإصدار لقانون الجرائم الإلكترونية خطى المشرع الفلسطيني خطوة هامة في سبيل مكافحة الجريمة، لكن في المقابل لم يأخذ المشرع بعين الاعتبار بعض الجوانب الهامة على صعيد مواجهة الجرائم الإلكترونية، لاسيما تلك منها المتعلقة بتنظيم وتصنيف هذه الجرائم، حيث خلى هذا القانون من أي تنظيم أو تصنيف محدد لها، الأمر الذي قد يثير بعض الإشكاليات العملية في تطبيقها، وعليه يمكن طرح إشكالية البحث في التساؤلات التالية: كيف نظم المشرع الفلسطيني أحكام الجرائم الإلكترونية؟ وما الأساس الذي استند إليه المشرع في وضعه للأحكام الخاصة بهذه الجرائم؟ وما هي خصوصية وأهمية الحق المعتدى عليه في وضع تصنيف دقيق للجرائم الإلكترونية في التشريع الفلسطيني؟

## أهداف البحث:

1. التعرف على الأسس والمعايير المختلفة لتصنيف الجرائم الإلكترونية.
2. بيان أهمية تصنيف الجرائم الإلكترونية في القانون الجنائي.
3. بيان أهمية تصنيف الجرائم الإلكترونية وفقا لطبيعة الحق المعتدى عليه.
4. التعرف على تصنيف وتنظيم أحكام الجرائم الإلكترونية في التشريعين الفلسطيني والإماراتي.

## منهجية البحث:

بهدف تحقيق النتائج والوصول إلى التوصيات المرجوة من هذه الدراسة اعتمد الباحث على المنهج المقارن والمنهج التحليلي لجمع المعلومات ذات العلاقة بموضوع البحث و تحليل الآراء الفقهية و بعض النصوص القانونية الواردة في القرار بقانون رقم (8) لسنة 2018 بشأن، بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته، وكذلك مقارنة هذه النصوص مع القانون رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الإماراتي

## تقسيم البحث:

**المطلب الأول: تصنيف الجرائم الإلكترونية وأهميته في القانون الجنائي.**

**المطلب الثاني: التنظيم القانوني للجرائم الإلكترونية في التشريعين الفلسطيني والإماراتي.**

# المطلب الأول:
# تصنيف الجرائم الإلكترونية وأهميته في القانون الجنائي

يشكل تصنيف الجرائم بشكل عام مسألة هامة على المستوى التشريعي والقضائي وكذلك بالنسبة للجهات المختصة في كشف وملاحقة مرتكبيها، لذا سنتناول موضوع هذا المطلب من ناحيتين نخصص لهما فرعين في الأول: أهمية تصنيف الجرائم الإلكترونية في القانون الجنائي والفرع الثاني: المعايير المختلفة لتصنيف الجرائم الإلكترونية وخصوصية الحق المعتدى عليه وأهميته في تصنيفها.

## الفرع الأول: أهمية تصنيف الجرائم الإلكترونية في القانون الجنائي

لتصنيف القواعد القانونية بشكل عام أهمية كبيرة في مجال العمل القانوني؛ فهو يسهل مهمة الباحثين المختصين في البحث عن حكم القانون لحل قضية قد تكون محل للنزاع،و يختصر الوقت والجهد على الباحثين عن حلول للمسائل القانونية المختلفة، و يعتبر كذلك من الوسائل الهامة لفهم المصطلحات الخاصة بقضية معينة، بالإضافة إلى مساهمته في ربط الظواهر الاجتماعية المتشابهة وإعطائها الوصف القانوني، فهو بمجمله عملية تسهل إيجاد الحلول القانونية لمختلف القضايا المتنازع عليها.(الحجار حلمي، و الحجار راني،2010، ص 51 وما بعدها)

وفي هذا المقام يقصد بتصنيف الجرائم: وضعها في مجموعة من الجرائم ضمن نظام موحد، يدخل فيه الأفعال الإجرامية بناءً على مجموعة من المعايير منها جسامة الجريمة أو طبيعة الحق المعتدى عليه،و شكل الجرم أو الفعل ومدة استمرارية النية الإجرامية، أو طبيعة القصد الجنائي ونوع الجريمة إلخ.(السراج،2018، ص 108 وما بعدها)

وفي إطار القانون الجنائي يشكل وضع تصنيف دقيق للجرائم مسألة في غاية الأهمية، يتمثل في إسباغ شيئاً من التنظيم والتبويب على مجموعة كبيرة من الجرائم التي ينظمها المشرع من خلال مجموعة من النصوص، مما يجعل التعامل معها والرجوع إلى أحكامها وفهمها أمر يتسم بالبساطة، ويشكل سهولة في تطبيقها والعثور فيها على الحلول الملائمة للقضايا القانونية، بالإضافة إلى أن ذلك يمكن الفرد العادي من فهم هذه النصوص، وبالتالي الالتزام بها وتوجيه سلوكه بما يتفق وأحكامها. (الفاضل، 1962،ص13ومابعدها)

ولعملية التصنيف بأهمية بالغة على مستوى دولي، لاسيما في مجال الإحصاء الجنائي الدولي، حيث أن وجود تصنيف دقيق للجرائم يساهم في وضع إحصائيات جنائية دولية دقيقة عن واقع الجريمة في دولة معينة، وبالتالي معرفة موقع الدولة على خارطة الإحصاء الجنائي، من حيث نوع وعدد الجرائم المرتكبة فيها، وكذلك يساهم في تعزيز تعاون الدول في مكافحة الجريمة.(Untied Nation Office On Drugs & CRIME 2015 p.p7-8)

وهناك جانب من الفقه الجنائي يرى أن تصنيف الجرائم الإلكترونية بناءً على وضع الجرائم بمجموعات لها خصائص متشابهة وعناصر مشتركة، على غرار الجرائم التقليدية، له أهمية بالغة في فهم حقيقة هذه الجرائم، ويقترح تصنيفها بناءً على دور الكمبيوتر في ارتكابها إلى دور سلبي وآخر إيجابي (Jahankhani، Nemrat &، Far، 2014 p154)

وبناءً على ما تقدم يرى الباحث أن تصنيف الجرائم وفق معايير دقيقة يجعل القوانين الخاصة بمكافحتها أكثر فعالية، كون عملية التصنيف تساهم في فهم حقيقة هذه الجرائم وبالتالي يسهل مهمة الجهات المختصة بملاحقة

مرتكبيها، وكذلك يضمن الوصول إلى تطبيق صحيح للقانون لاسيما في مرحلة التحقيق الابتدائي الذي يؤسس للاتهام بناءً على تكييف الواقعة الجرمية ومرحلة المحاكمة التي تبنى على فحص الأدلة التي بني عليها تكييف سلطات التحقيق وإصدار الحكم

## الفرع الثاني: المعايير المختلفة لتصنيف الجرائم الإلكترونية وخصوصية الحق المعتدى عليه وأهميته في تصنيفها

نظراً لأهمية موضوع تصنيف الجرائم الإلكترونية ظهرت العديد من المعايير بهدف وضع تصنيف محدد لهذه الجرائم، إلا أن مسألة الاتفاق على حل هذه المشكلة لا تزال تواجه صعوبات كبيرة. وعليه سنحاول في هذا الجزء من البحث الوقوف على الكيفية التي حاول المختصين وفقه القانون الجنائي الاجتهاد لوضع تصنيف محدد للجرائم الإلكترونية، وذلك من خلال تناول أهم التصنيفات والأسس التي استندت إليها على النحو الآتي:

### أولا: الأسس والمعايير المختلفة لتصنيف الجرائم الإلكترونية.

تتميز التصنيفات التي وضعت للجرائم الإلكترونية بتنوعها واختلاف الأسس والمعايير التي استند إليها الفقهاء والمختصين لهذه الجرائم إلى مجموعات، وهذا بطبيعة الحال ناجم عن تنوع المجالات التي بدأت ترتكز على الاستخدامات المختلفة للتقنيات الحديثة

فهناك إجماع بين فقهاء القانون والمختصين على أن الجرائم الإلكترونية ليست محصورة في فئة أو نوع واحد، وأن هناك اختلاف في التصنيفات التي وضعت لها، وذلك يرجع إلى الاختلاف في وجهات النظر حول أسس تصنيف هذه الجرائم؛ فالبعض استند إلى معيار دور الحاسوب في الجريمة، والبعض الأخر صنفها بناءً على أسلوب ارتكابها، وهناك من صنفها بناءً على الباعث على ارتكابها، وأخيراً هناك من صنفها استنادا إلى تنوع طبيعة الحق المعتدى عليه إلى جرائم أموال وجرائم تنتهك حرمة الحياة الخاصة.(توبة،2009، ص131)

وفي هذا المقام سنتعرض لأهم التصنيفات التي وضعت للجرائم الإلكترونية على النحو الآتي:

ذهب جانب من فقه القانون الجنائي في تصنيفه للجرائم الإلكترونية إلى الاستناد لمعيار موطن الاختراق وكذلك معيار مدى مساس هذه الجرائم بالأشخاص والأموال حيث تم تقسيمها على النحو الآتي:

أ- معيار موطن الاختراق: فبموجب هذا المعيار صنفت الجرائم الإلكترونية إلى جرائم اختراق الأمن المادي وجرائم اختراق الأمن الشخصي والحماية الخاصة بالاتصالات وعمليات الحماية

ب- معيار مساس هذه الجرائم بالأشخاص والأموال: وصنفت إلى جرائم تستهدف الأشخاص وتشمل الجرائم غير الجنسية و كذلك جرائم الأموال باستثناء السرقة.( أشار إليه يوسف،2008،ص. 56)

وفي هذا الإطار صنفت جرائم الكمبيوتر في مؤتمر الأمم المتحدة الثالث لمنع الجريمة والعدالة الجنائية بحيث تضم الفئات التالية:

1. الأفعال التي تكون فيها البيانات أو النظم الحاسوبية هي الشيء المستهدَف بالجرم، ومنها ما يُرتكب من جرائم بحقِّ سرِّية البيانات أو النظم الحاسوبية وسلامتها وتَوأفرها، مثل أفعال الاقتحام غير المشروع للبيانات و الحاسوبية.
2. الأفعال التي تشكِّل فيها النظم أو المعلومات الحاسوبية جزءًا أساسيا من وسائل لارتكاب هذه الجرائم، ومنها استخدام البيانات أو النظم الحاسوبية لأغراض الاحتيال أو السرقة أو إلحاق الأذى بالآخرين، وكذلك الجرائم

المتصلة بالحاسوب ومحتوى الإنترنت والجرائم المتعلقة بالهوية.( مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، قطر نسيان 2015،ص.8)

وتبعا لدور جهاز الحاسوب فيها، صنفت الجرائم الإلكترونية إلى ثلاث فئات رئيسية تشمل فئة جرائم القرصنة التي يكون الكمبيوتر فيها هدف للنشاط الإجرامي، وفئة جرائم الاحتيال عبر الإنترنت: استخدام الكمبيوتر كأداة فقط حتى يمكن تنفيذ النشاط الإجرامي تخزين البيانات: بالنسبة لهذا النوع من النشاط الإجرامي، يكون استخدام الكمبيوتر عرضيًا للجريمة. (Brenner & Sukhai N،Lewis,مشار إليه في Raghavan & Parthiban 2014 p. 3)

وهناك تصنيف آخر يستند على أساس الفصل بين جرائم الكمبيوتر وجرائم الإنترنت حيث يقوم هذا الفصل على معيار التمييز بين الأفعال التي تستهدف المعلومات في نطاق الكمبيوتر في مراحل والتخزين والمعالجة والاسترجاع، والأنشطة التي يكون هدفها الشبكات ذاتها أو المعلومات المنقولة عبرها والأنشطة التي تستهدف مواقع الإنترنت وخوادمها من نظم الكمبيوتر الكبيرة أو تلك التي يكون هدفها تطبيقات واستخدامات وحلول الإنترنت وما نشأ في بيئتها من أعمال إلكترونية وخدمات (توبة 2009،ص 139)

كما اعتمد البعض على الهدف من ارتكاب الجريمة كمعيار لتصنيف هذه الجرائم، حيث قسمها إلى ثلاثة مجموعات،مجموعة الجرائم التي تستهدف النظام والمعلومات، ومجموعة تستهدف مستخدمي الكمبيوتر بهدف ارتكاب جرائم أخرى، وأخيرا مجموعة الجرائم التي تمس محتوى الموقع الإلكترونية. (مدني سالم، مشار إليه لدى محمد 2015،ص 35)

وبالاستناد إلى طبيعة الحق المعتدى عليه صنفت الجرائم الإلكترونية، من خلال تقسيمها إلى عدة أقسام؛ قسم يكون فيها موضوع الجريمة الاحتيال المعلوماتي، وقسم آخر يكون موضوع الجريمة فيه التعرض لحرمة الحياة الخاصة، وأما القسم الأخير يكون موضوعها التخريب والتعدي على برامج الحاسب الآلي والمعلومات (علكوم، وليد 2000)

وفي الاتجاه نفسه ذهب بعضهم إلى تصنيف هذه الجرائم الى مجموعة من الفئات بحيث تجمع كل منها أنواع معينة من الجرائم على النحو الآتي:»

1. فئة الجرائم عامة: و تشمل الأخطاء المتعمدة للأداء وإغفال الواجب، التجاهل، التهور والطيش، التآمر والتواطؤ
2. فئة الجرائم المادية: منها السرقة، التدمير والإتلاف، تزييف المستندات، التعدي على الممتلكات.
3. فئة الجرائم اقتصادية: الاحتيال والاختلاس الرشوة، والابتزاز و انتهاك المراسلات الاقتصادية، التزييف والتزوير
4. فئة الجرائم المرتكبة ضد الأشخاص، بحيث تشمل جرائم القذف والتشهير، تسهيل الدعارة، انتهاك الخصوصية، الإهانة، التحرش الجنسي، الخطف، القتل، الانتحار." ( داوود،أشار إليه نصار،2017 ص 13)

وتجدر الإشارة إلى أن تصنيف الجرائم تبعا لنوع المعطيات وطبيعة الحق المعتدى عليه، هو التصنيف الذي تزامن مع البدء في ظهور التشريعات التي وضعت لمكافحة الجريمة الإلكترونية، وهو يرتبط بالتطور التاريخي لهذه الظاهرة، وفقاً لهذا المعيار تم تقسيم هذه الجرائم إلى جرائم واقعة على ذات المعطيات، والثانية الجرائم الواقعة على ما تمثله المعطيات المعالجة من أموال وأصول(توبة 2009،ص135)

وفي هذا الإطار يرى بعض المختصين أن تقسيم الجرائم الإلكترونية على أساس وسيلة ارتكاب الجريمة وجرائم ومحتوى يعبر عن الاتجاه الذي تتبعه التدابير التشريعية في أوروبا، حيث أن أفضل ما أظهر هذا التقسيم هو الاتفاقية الأوربية لجرائم الكمبيوتر والإنترنت عام 2001، حيث تم وضع إطار عام لتصنيف جرائم الكمبيوتر والإنترنت، بهدف وضع قائمة تتضمن الحد الأدنى كمحل للتعاون الدولي في حقل مكافحة الجرائم الإلكترونية، حيث أوجدت هذه الاتفاقية تقسيما تضمن أربع طوائف رئيسية لجرائم الكمبيوتر والإنترنت (يونس، أشار إليه المردني، 2022،ص15)

وبموجب التقرير التفسيري لاتفاقية بودابست قسمت أحكام الجرائم الإلكترونية إلى أربعة فصول تضمن كل فصل منها مجموعة النصوص القانونية، حيث تناولت الفصل الأول التعريف بالمصطلحات المستخدمة فيها، وفي الفصل الثاني نصت على مجموعة الأحكام الوضعية والإجرائية الخاصة بالجرائم الإلكترونية، وفي الفصل الثالث أحكام التعاون الدولي، وفي الأخير أحكام ختامية( التقرير التفسيري لاتفاقية الجرائم المعلوماتية 2001،ص3)

وأما فيما يتعلق بالأحكام الموضوعية للجرائم المعلوماتية فقد صنفت الاتفاقية المذكورة الجرائم إلى المجموعات التالية:( التقرير التفسيري لاتفاقية الجرائم المعلوماتية 2001)

**المجموعة الأولى:** جرائم ضد السرية والنزاهة والدخول إلى أنظمة المعلومات، وتشمل الدخول غير المشروع، والتصنت والاعتراض والتدخل في البيانات و أنظمة المعلومات

**المجموعة الثانية:** تشمل الجرائم المتصلة باستخدام الكمبيوتر، كجرائم التزوير والاحتيال.

**المجموع الثالثة:** وهي الجرائم المتعلقة بمحتوى البيانات، وتتضمن جرائم نشر وتوزيع وإنتاج ونقل وامتلاك الأعمال الإباحية المتعلقة بالأطفال

**المجموعة الرابعة:** احتوت على الجرائم المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة لها

وبموجب البروتوكول الملحق باتفاقية بودابست تم إضافة مجموعة أخرى من جرائم الكمبيوتر وهي الجرائم ذات صلة بنشر المعلومات ذات الطابع العنصري والحض على استخدام القوة ضد شخص أو مجموعة من الأشخاص والتميز وغيرها من أشكال التمييز العنصري( البروتوكول الملحق باتفاقية بودابست 2002 )

ولابد لنا من الإشارة في هذا المقام إلى أن هناك جانب من المختصين اعتبر تصنيف الجرائم الإلكترونية وفقا لمعيار نوع المعطيات وكذلك تبعا لدور الحاسب الآلي في ارتكابها، ومساسها بالأشخاص والأموال من أهم التصنيفات التي وضعت بشأن هذا النوع من الإجرام المستحدث (فتيح، ورعد 2017ص502)

وهناك جانب أخر صنف هذه الجرائم إلى صنفين معتمدا على معيار تاريخي مرتبط في زمن ظهور هذه الجرائم، فاعتبر جزء من هذه الجرائم جرائم تقليدية موجود قبل عصر المعلومات لكنها أصبحت ترتكب بواسطة وسائل تكنولوجية. كما صنف على أساس جرائم مستحدثة تزامن ظهورها مع عصر المعلومات حيث لم تكن معروفة قبل هذا العصر لاسيما فترة اختراع الإنترنت.(الغافري، مشار إليه في الخن، 2018، ص 27)

وفي واقع الأمر وبالرغم من تعدد التصنيفات التي وضعت للجرائم الإلكترونية، فأنها لم تصل إلى مرحلة وضع تصنيف نهائي ومتفق عليه بل قد يتجاوز الأمر هذه التصنيفات بظهور تصنيفات جديدة؛ هذا يعود بشكل أساسي إلى استمرار التطور الحاصل في حقل تكنولوجيا المعلومات وزيادة اعتماد الإنسان على هذا القطاع وما يترتب عليه من تطور الجريمة ووسائل ارتكابها(توبة، 2009، ص139)

فالتصنيفات السابقة التي وضعها فقه القانون الجنائي والمختصين والاتفاقيات الخاصة بشأن جرائم الحاسوب والإنترنت، انطلقت من معايير مختلفة في محاولة لإيجاد حل مشكلة تصنيف هذه الجرائم، فمنهم من صنفها استنادا إلى طبيعة الحق المعتدى عليه، وصنفت لدى آخرين استنادا إلى دور الحاسوب فيها، بينما تم تصنيفها لدى البعض تبعا لمساسها بالأشخاص والأموال.

وبهذا الصدد يرى الباحث أن مسألة تصنيف الجرائم المرتبطة بالحاسوب والإنترنت قد تكون أكثر دقة من خلال اختيار الجرائم ذات الطبيعة الخاصة منها وتصنيفها في مجموعة واحدة، ومن ثم وضع تصنيف شامل يتعلق بكل مجموعة من الجرائم التي تقع باستخدام تكنولوجيا المعلومات والتي تتشابه خصائصها والتي ترتكب عن طريق الكمبيوتر والإنترنت مثل: مجموعة الجرائم الواقعة على الأشخاص، مجموعة الجرائم الواقعة على أمن الدولة، مجموعة الجرائم الواقعة على الاقتصاد أو التي تقع على الحقوق والحريات العامة للمواطن والإنسان، أو تلك التي تستهدف المحتوى المحفوظ أو الذي يتم نقله أو نشره بإحدى وسائل التقنية الحديثة

وعليه استخلاصا لما سلف ونظراً لأهمية مسألة تصنيف الجرائم في القانون الجنائي،كمسألة لها دور أساسي في التطبيق الصحيح لهذا القانون،بالإضافة إلى كونها من المسائل الهامة في التكييف القانوني للوقائع في الدعوى الجزائية والتي يبنى عليها تحقيق المحاكمة العدالة، يجب أن يتم تصنيفها على أساس علمي صحيح، ضمن معايير واضحة ودقيقة تساهم في فهم حقيقتها وبالتالي تساهم في فعالية مكافحتها.

## ثانيا: خصوصية الحق المعتدى عليه وأهميته في تصنيف الجرائم الإلكترونية

تسير أغلب التشريعات الجزائية الحديثة على منهج تنظيم الجرائم المتشابهة استنادا على معيار طبيعة الحق المعتدى كأساس لتصنيف الجرائم، حيث ينظم المشرع الجرائم ضمن مجموعات مستقلة ويضعها تحت عناوين مستقلة، فتصنيف الجرائم بشكل عام في القسم الخاص من قانون العقوبات يتم وفق أسس علمية تقوم على منهج يتم من خلاله تصنيف الجرائم استناد إلى العناصر التي تجمعها في إطار التشابه الحاصل بينها وهذا يستند بطبيعة الحال إلى خصوصية الحق المعتدى عليه.(عبيد، 2018، ص4).

إن طبيعة الحق المعتدى قد تكون العنصر المفترض لقيام بعض الجرائم، حيث يشترط المشرع وجوده لتحقق أركان جريمة معينة ووقوعها على مصلحة محددة، وبالتالي يصبح وقوع الفعل الإجرامي على هذه المصلحة عنصرا يدخل ضمن عناصرها القانونية التي يعتبر وجودها من الوقائع التي تدخل في عملية التكييف القانوني للجريمة (أبو جامع،2016، ص49).

وتظهر كذلك أهمية الحق المعتدى في التنظيم القانوني لمكافحة الجريمة في مراحل مختلفة تبدأ من وجود النص الجنائي وتنتهي بإلغائه أو تعديله، فمن ناحية تشريع النص الجنائي وهي مرحلة إضفاء صفة التجريم على سلوك معين، يشكل الحق المعتدى عليه الأساس الذي ينطلق منه المشرع للتجريم وتحديد نطاقه وكذلك النموذج القانوني لأي جريمة وظروفها، ومن ناحية تطبيق هذا النص، للحق المعتدي عليه أهمية في تفسيره وحل الإشكالية المرتبطة بتنازع نصوص القانون الجنائي، كما للحق المعتدى عليه أهمية مستقبلية ترتبط بوجوده من حيث إلغائه أو تعديله (البياتي 2002،ص 56ومابعدها)

كما أن لطبيعة الحق المعتدى عليه أهمية من ناحية إجرائية، حيث يشكل في بعض الأحيان يشكل الأساس لتحريك الدعوى الجزائية من عدمه، فالمشرع الفلسطيني في قانون الإجراءات الجزائية اعتبر عدم أهمية محل الدعوى سببا يبرر للنيابة العامة اتخاذ قرار حفظ أوراق الدعوى الجزائية(المادة 152 قانون الإجراءات الجزائية الفلسطيني ).

وتزداد أهمية الاستناد إلى طبيعة الحق المعتدى في تصنيف الجرائم الإلكترونية؛ وذلك كونه من نواحي عدة منها: يشكل الخاصية الأهم التي يمكن الاعتماد عليها لوضع تصنيف دقيق لها؛ بالإضافة إلى موضوع الاعتداء في هذه الجرائم هو الذي يميزها عن غيرها من الجرائم التقليدية، فطبيعة محل الاعتداء في الجريمة الإلكترونية يرد على المعلومات والبرامج التي تعتبر بمثابة نبضات إلكترونية، بالإضافة إلى أن محلها هو الذي وضع هذه الجرائم ضمن دائرة الإجرام المستحدث.(باطلي 2015، ص 33).

فالمعلومات التي تقع عليها الجريمة الإلكترونية حسب رأي الفقه الحديث، ما هي إلا تعبير عن مجموعة من القيم المستحدثة القابلة للاستئثار، بمعزل عن الدعامة المادية المثبتة عليها، والتي يمكن تقديرها بالمال ويكمن أن يكون لها قيمة اقتصادية (vivant & Catala، مشار إليه في صالح، وأنيسة 2015،ص17)

ومن زاوية أخرى تظهر خصوصية الحق المعتدى عليه في الجرائم الإلكترونية، باحتمال تعدد محل الاعتداء فيها، وبالتالي تعدد أوصافها القانونية، فالجريمة الإلكترونية قد تقع على مال مادي أو معنوي، فمن ناحية الطبيعة المادية لمحلها يظهر بالاعتداء على معلومات في صورة مادية مخزنة على دعامة الكرتونية، وأما الصورة المعنوية لهذا المحل تتمثل عندما تكون المعلومات هدف لهذه الجريمة وهي حال انتقال أو مخزن في ذاكرة النظام (ممدوح، مشار إليه في العجمي 2014، ص 25)

كما يفيد هذا التصنيف بشكل أو باخر في التوصل إلى مرتكب هذه الجرائم بناءً على الربط بين محل الاعتداء والباعث على ارتكابها؛ انطلاقا من أن المجرم المعلوماتي وعلى غرار المجرم التقليدي يحركه دوافع معينة لارتكابها، فقد يكون الانتقام أو التعلم أو الحصول على المال، ولعل المكسب المادي يعتبر من أهم هذه الدوافع، والرغبة بتحقيق الثراء هو الهدف الذي يسعى الجاني من خلال ارتكاب هذه الجرائم في أغلب الأحيان؛ وذلك يعود إلى سهول ارتكابها والأرباح الكبيرة التي قد تنتج عنها (الملط خليفة، أشار إليه صالح، وأنيسة 2015،ص30)

ومن جهة أخرى يمكن القول أن لتصنيف الجرائم الإلكترونية بناءً على معيار طبيعة الحق المعتدى عليه، أهمية عملية وعلمية، من ناحية الفقه الجنائي وكذلك في مجال العمل الأكاديمي في التدريس الجامعي، حيث أن تصنيفها وفق لهذا المعيار، يمكن الفقه الجنائي من القيام بإجراء البحوث والشروحات والتفسيرات لمجموعة أو فئة معينة من الجرائم الإلكترونية باعتبار مجموعة ترتبط بأحكام عامة معينة ولكنها تختلف بأركانها الخاصة، ويساهم كذلك في سهول إدراج هذه الجرائم ضمن الخطط الدراسية في كليات الحقوق

ولهذا التصنيف بعد أخر يتعلق بمسألة الوقاية من الجرائم الإلكترونية، حيث أن تصنيفها وفق لهذا المعيار من خلال ربطها بموضوع حماية حق أو مصلحة معينة ووضع عنوان أو مسمى لهذه الجرائم ضمن قانون الجرائم الإلكترونية، يسهل إجراءات الوقاية من مخاطرها داخل المجتمع، إذ أن طبيعة هذه الجرائم من حيث ارتباطها بمسائل تقنية يصعب على الإنسان العادي فهم خطورتها، وبالتالي إعطاء عنوان لها وربطها بحق معين يساهم في الجانب الوقائي من خطورة هذه الجرائم

وعلاوة على ذلك أن لتصنيف الجرائم الإلكترونية وفق طبيعة الحق المعتدى عليه له دور هام في مجال

التحقيق وإثبات هذه الجرائم، فالجرائم الإلكترونية من الجرائم ذات خصوصية مرتبطة في صعوبة إثباتها وذلك يعود لطبيعة محل الاعتداء فيها، وكذلك وسائل ارتكابها واتساع مسرح الجريمة فيها، حيث أن تحديد ومعرفة طبيعة الحق المعتدى عليه من طرف الجهات القائمة على التحقيق يساهم في تحديد طبيعة الآثار والأدلة التي يجب البحث عنها وكذلك تحديد مسرحها وحصر أماكن وجودها

ويرى الباحث كذلك أنه ومن أجل الوصول إلى تصنيف صحيح للجرائم الإلكترونية وتجنب الوقوع في التكيف الخاطئ لهذه الجرائم، يتطلب تحديد المصلحة الاجتماعية التي وقع عليها الاعتداء، وكذلك معرفة هل هذه المصلحة محمية في إطار قواعد القانون الجنائي. فالمصلحة الجديرة بالحماية الجنائية من خلال تشريعات مكافحة الجرائم الإلكترونية هي حماية الأجهزة التقنية بمختلف أنواعها بالإضافة إلى حماية المعلومات والبيانات المخزنة عليها، وكذلك التي يتم تداولها من خلال الشبكات

وخلاصة القول في هذا الجانب أن وضع تصنيف دقيق وواضح للفعل المرتكب يعني نسبته أو إلحاقه بمجموعة معينة من الجرائم التي يجمعها وحدة محل الاعتداء،وعليه فإن تصنيف الجرائم الإلكترونية وفق طبيعة الحق المعتدى عليه يساهم بشكل كبير في الوصول إلى تكييف قانوني صحيح لمختلف الجرائم التي تقع من خلال الإنترنت واستخدام التقنيات الحديثة بمختلف أنواعها.

# المطلب الثاني
# تنظيم وتصنيف الجرائم الإلكترونية في التشريع الفلسطيني والإماراتي

يعتبر قانون الجرائم الإلكترونية من القوانين العقابية الخاصة التي نظم فيها المشرع أحكام جرائم ذات خصوصية معينة تميزها عن الجرائم الأخرى، لذا فأن مسألة تبويب وتصنيف هذه الجرائم تحتل مكانة هامة في مجال العمل القانوني، فالقسم الخاص من قانون العقوبات وكذلك القوانين العقابية الخاصة تطبق في الأساس على الجرائم التي ترتكب في مجال العلاقات الاجتماعية والاقتصادية والسياسية والأمنية وهي علاقات بطبيعتها قابلة للتطور، التي بمجملها تستدعي بشكل مستمر تطوير التشريع الجنائي لمواجهة ما يستحدث من جرائم في إطار هذه العلاقات

وعليه ونظراً للأهمية القصوى التي يحتلها موضوع تصنيف وتنظيم الجرائم، سنخصص لموضوع هذا المطلب فرعين: في الأول تنظيم وتصنيف أحكام الجرائم الإلكترونية في التشريع الفلسطيني، وفي وأما الفرع الثاني نخصص لموضوع تنظيم وتصنيف أحكام الجرائم الإلكترونية في قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي

## الفرع الأول: تنظيم وتصنيف الجرائم الإلكترونية بالتشريع الفلسطيني

قبل البدء في الخوض في مسألة الكيفية التي نظم بها المشرع الفلسطيني أحكام الجرائم الإلكترونية لابد لنا الإشارة إلى الاطار القانوني الناظم لمكافحة هذه الجرائم في فلسطين، ويشمل مجموعة من التشريعات، من ضمنها القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية، و قانون الاتصالات رقم (3) لسنة 1996. بالإضافة إلى إحالة المشرع للتشريعات الجنائية السارية في فلسطين لاسيما قانون العقوبات الأردني رقم 16 لسنة 1960 النافذ في الضفة الغربية و قانون العقوبات (رقم 74) لسنة 1936 النافذ في قطاع غزة، وبعض القوانين الخاصة كالقرار بقانون رقم (18) لسنة 2015م بشأن مكافحة المخدرات والمؤثرات العقلية، والقرار بقانون رقم (39) لسنة 2022م بشأن مكافحة غسل الأموال وتمويل الإرهاب، ولقرار بقانون رقم (6) لسنة 2017 م بشأن تنظيم نقل وزراعة الأعضاء البشرية

وفي هذا المقام تجدر الإشارة إلى أن المشرع الفلسطيني أحال صراحة إلى تطبيق بعض أحكام هذه القوانين على الجرائم الإلكترونية، حيث اعتبر و لغايات التجريم في قانون الجرائم الإلكترونية أي جريمة تمت في تشريع آخر تمت بأداة الإلكترونية وبأسلوب الإلكتروني، بالإضافة إلى النص على تطبيق أي عقوبة أشد منصوص عليها في القوانين العقابية السارية أو أي قانون آخر (المواد 17، 18، 19، 44، 45) من قانون الجرائم الإلكترونية الفلسطيني[1]

وعليه يعتبر القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته، هو القانون الأساسي الخاص بمكافحة الجرائم الإلكترونية في فلسطين حيث يتكون هذا القانون من 57 مادة وهو غير مقسم إلى أي نوع من أنواع التقسيمات أو التبويب أو غيره

1 أينما وردت الإشارة لقانون الجرائم الإلكترونية الفلسطيني، يقصد به القرار بقانون رقم (10) لسنة 2018م بشأن الجرائم الإلكترونية وجرائم الاتصالات وجرائم تكنولوجيا المعلومات وتعديلاته
وتجنبا لتكرار ذكر مسى هذا القانون تجدر الإشارة إلى أن جميع النصوص المشار إليها في الفرع الأول من المطلب الثاني، يعتبر مصدرها قانون الجرائم الإلكترونية الفلسطيني

وهذا تجدر الإشارة إلى أن هذا القانون خضع للتعديل مرتين وذلك بموجب القرار بقانون رقم (28) لسنة 2020م، حيث خص المشرع بهذا التعديل المادة (15) من القانون الأصلي وهي التي تضمنت أحكام الابتزاز الإلكترونية وتناول المشرع في التعديل العقوبة المقررة على هذه الجريمة باتجاه التشدد في عقوبة الحبس والغرامة المالية المفروضة على مرتكبها. وكما عدل هذا القانون بموجب القرار بقانون رقم (38) لسنة 2021 م، حيث انصب التعديل الأخير على العديد من الأحكام الموضوعية والإجرائية، بالإضافة إلى تعديل عنوان القانون الأصلي ليصبح قرار بقانون بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات، وكذلك إضافة العديد من النصوص القانونية التي تجرم بعض الأفعال المرتكبة في قطاع الاتصالات والمعلومات، لاسيما تلك التي تقع في مجال تقديم الخدمات وكذلك إدارتها ومخالفة الشروط المتعلقة بها، بالإضافة إلى تشديد العقوبات على بعض الجرائم وإضافة مجموعة من التعريفات لبعض المصطلحات الواردة فيه وغيرها من الأحكام.

وبالرجوع إلى أحكام قانون الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات الفلسطيني والذي نظم فيه المشرع أحكام هذه الجرائم نلاحظ أن المشرع وضع في صادرة هذا القانون مجموعة التعريفات، حيث نص في المادة (1) منه على معاني المصطلحات الواردة فيه، وفي المادة (2) حدد المشرع النطاق المكاني والشخصي والعيني لتطبيق قانون الجرائم الإلكترونية الفلسطيني

وبموجب أحكام هذا القانون حدد المشرع الجهات المختصة في ملاحقة مرتكبي الجرائم الإلكترونية، حيث في المادة (3) على إنشاء وحدة متخصصة في الشرطة الفلسطينية وقوى الأمن من مأموري الضبط القضائي، تسمى (وحدة الجرائم الإلكترونية ) وأسند الإشراف القضائي على هذه الوحدة للنيابة العامة، كما حدد صلاحية القضاء المختصة في النظر في الدعوى الجزائية الناتجة عن هذه الجرائم حيث جعل ذلك من مهمة القضاء النظامي والنيابة العامة.

ويلاحظ أن المشرع الفلسطيني عمل على مواكبة التطور الذي حصل على صعيد مكافحة الجرائم الإلكترونية عندما نص على إنشاء وحدة متخصصة لملاحقة مرتكبي هذه الجرائم، لكن في المقابل جانبه الصواب في موقع تنظيم هذه المسألة، فالملاحقة الجزائية تعتبر مسألة إجرائية يجب تضمينها في الأحكام الإجرائية لملاحقة هذه الجرائم، لاسيما أن المشرع في نهاية قانون الجرائم الإلكترونية نص على العديد من المسائل الخاصة بتنظيم الأحكام الإجرائية المتعلقة بملاحقة مرتكبي الجرائم المنصوص عليها في هذا القانون

وأما بالنسبة للأحكام الموضوعية التي تضمنها هذا القانون و لغايات البحث سنتطرق بشكل موجز لمجموعة الجرائم التي نص عليها المشرع الفلسطيني في قانون الجرائم الإلكترونية وذلك من اجل التعرف على الأساس الذي نظم فيها المشرع أحكام هذه الجرائم وذلك على النحو التالي:

1. الدخول العمد وغير المصرح به إلى نظام معلوماتي أو موقع إلكتروني أو تجاوز الدخول غير المصرح أو استمر بالتواجد رغم علمه بأن لا حق له بالتواجد (المادة: 4)

2. إعاقة أو تعطيل الوصول إلى الخدمة أو الأجهزة والبرامج أو مصادر البيانات أو المعلومات بواسطة الشبكة الإلكترونية أو احدى وسائل تكنولوجيا المعلومات

3. تعطيل أو إيقاف الشبكة الإلكترونية أو أتلاف البرامج أو تعطيلها.(المادة: 6)

4. التقاط المعلومات المرسلة خلال الشبكة أو قام بتسجيلها والتنصت على المعلومات المرسلة، وكذلك فك البيانات المشفرة دون وجه حق والانتفاع من الخدمة بوجه غير مشروع. (المواد: 7، 8، 9)

5. أنشاء شهادة أو تقديم بيانات غير صحيحة عن هويته للجهات المختصة، وتزوير المستندات الإلكترونية واستعملها. (المواد 10،11)

6. استخدام شبكة الإنترنت أو سائل تكنولوجيا المعلومات للوصول بطريقة غير مشروع إلى بيانات أو أرقام وسائل التعامل الإلكترونية أو التلاعب بها. (المادة: 12)

7. سرقة الأموال واختلاسها وكذلك الاحتيال باستخدام الشبكة الإلكترونية أو وسيلة من وسائل تكنولوجيا المعلومات، وجرم استعمال الشبكة أو احدى وسائل تكنولوجيا المعلومات للقيام بابتزاز شخص أو تهديده(المواد 13، 14، 15)

8 الترويج للأعمال الإباحية، وتجارة المخدرات والمؤثرات العقلية والترويج لها وكذلك تجريم تجارة الأعضاء البشرية وغسل الأموال باستخدام الشبكة الإلكترونية أو وسائل التعامل الإلكترونية. (16، 17، 18، 19)

بالإضافة إلى ما سبق ذكره أورد المشرع العديد من الأحكام الموضوعية في (المواد 20،21،22) تتعلق بتجريم انتهاك الملكية الفكرية والصناعية، وعدم احترام الحق في التعبير وحرية الرأي بمختلف الوسائل المرئية والمسموعة حرية القول والنشر وغيرها من الحقوق المرتبطة بحرية التعبير، بالإضافة إلى حماية الحق في الخصوصية وحرمة الحياة الخاصة وتجريم التدخل التعسفي بها من خلال استخدام الشبكة الإلكترونية أو التطبيقات المختلفة.

كما جرم المشرع الفلسطيني في قانون الجرائم الإلكترونية إنشاء المواقع أو الحسابات الإلكترونية أو نشر المعلومات بقصد الترويج لإدارة مشروع مقامرة أو التسهيل له، وكذلك تجريم المواقع والحسابات لنشر أو الترويج للسلوكيات والأفكار التي تؤدي إلى إثارة الكراهية وأثارة النعرات الدينية والطائفية أو التبرير لأعمال الإبادة الجماعية أو الجرائم ضد الإنسانية و حيازة أي من وسائل تكنولوجيا بغرض الاستخدام أو حيازة بيانات أو كلمات سر أو وإنتاج البرامج والتطبيقات أو استردادها أو و روج لها بغرض ارتكاب أي من الجرائم المنصوص عليها في هذا القانون

و تضمن هذا القانون العديد من الأحكام الخاصة بظروف ارتكاب بعض الجرائم الإلكترونية، من ناحية التشديد أو الإعفاء،ومن أهم ظروف التشديد التي حددها المشرع ما نص عليه صراحة في المواد(27،4، 51،52)

وأما فيما يتعلق في ظروف الإعفاء من العقوبة فقد نص المشرع في المادة (53) على حالة إعفاء الجناة وحدد شروط تطبيق هذه الحالة، كما أجاز المشرع للمحكمة بموجب هذا النص أن تقضي بوقف تنفيذ العقوبة في حال حصل الإبلاغ بعد علم السلطة المختصة، وأدى إلى ضبط باقي الجناة

ويلاحظ من خلال النص المذكور أعلاه أن المشرع الفلسطيني خرج عن سياسته الجنائية المتبعة في الإعفاء والتخفيف، فلم ينص على أي ظرف مخفف للعقوبة في قانون الجرائم الإلكترونية وهو النهج المتبع للمشرع في بعض القوانين العقابية الخاصة كقانون مكافحة الفساد، والتي نص فيه أن الجاني يستفيد العذر المخفف في حال حصل الإبلاغ بعد علم السلط المختصة، بجريمة فساد وأدى إلى ضبط باقي الجناة. ومتحصلات الجريمة هذا ما أورده صراحة في المادة (25) من قانون مكافحة الفساد ولم ينص على وقف تنفيذ العقوبات كما هو الحال في قانون الجرائم الإلكترونية.

وإضافة إلى ما سبق ذكره فإن المشرع الفلسطيني نظم أحكام حالات وقف تنفيذ العقوبة في قانون الإجراءات الجزائية بحيث تطبق على جرائم محددة، حيث يكون الحكم بإيقاف تنفيذ العقوبة في جناية أو جنحة بالغرامة أو بالحبس مدة لا تزيد على سنة (المادة: 284).،بينما لم يشر إلى هذا الشروط في قانون الجرائم الإلكترونية للاستفادة المحكوم من وقف تنفيذ العقوبة

وفي هذا الصدد ومن أجل تحقيق الانسجام التشريعي بين النصوص القانوني يرى الباحث ضرورة قيام المشرع بتوحيد سياسته الجنائية المتعلقة بشروط الاستفادة من نظام وقف تنفيذ العقوبة، والاكتفاء بالتنظيم

الموجود لهذا الأجراء في قانون الإجراءات الجزائية الفلسطيني، الذي نظم أحكام هذا النظام بشكل مفصل بجميع مراحله والآثار المترتبة عليه.

وأما فيما يتعلق بأحكام التحريض أو المساعدة أو الاتفاق على ارتكاب جريمة والشروع في ارتكاب جريمة من الجرائم المنصوص عليها في قانون الجرائم الإلكترونية، ساوى المشرع في العقابية على الأفعال المذكورة والعقوبة المقررة للفاعل الأصلي، هذا ما نص عليه صراحة في المادة 28 من قانون الجرائم الإلكترونية وجرائم تكنولوجيا الاتصالات والمعلومات

وبذلك نجد أن المشرع الفلسطيني خرج عن القواعد العامة الواردة في القانون الجنائي فيما يتعلق في تحديده للمسؤولية الجنائية في حال المساهمة الجنائية، حيث ساوى في العقوبة بين كل من ساهم في ارتكاب جريمة إلكترونية بغض النظر عن نصيب مساهمته في الجريمة، بالإضافة إلى النص على العقاب على الشروع في الجنح كأصل عام وثابت

ويرى الباحث أن النهج الذي اتبعه المشرع الفلسطيني في سياسته الجنائية في التشدد في أحكام المسؤولية الجنائية يتماشى مع خطورة هذه الجرائم وطبيعتها من حيث اتساع مسرح الجريمة وصعوبة إثباتها وكذلك خطورة مرتكبيها

وأما فيا يتعلق بالأحكام الإجرائية فقد تضمن هذا القانون في طياته بعض الأحكام الإجرائية المتعلقة بملاحقة مرتكبي الجرائم الإلكترونية حيث خصص لهذا الهدف مجموعة من النصوص القانونية التي نظمت إجراءات الملاحقة وجمع الأدلة والمحافظة عليها وتحديد نوع الأدلة التي تقبل إثبات هذه الجرائم، وكذلك سبل التعاون الدولي في مواجهة هذه الجرائم، والمسؤولية المترتبة على إفشاء الأسرار الخاصة بالإجراءات المنصوص عليها والعبث في الأدلة، وكذلك ألزم المشرع مزودي الخدمة بتزويد الجهات المختصة بالملاحقة بكل المعلومات المتعلقة بالجريمة، وأوجب على الأجهزة الحكومية ومؤسسات الدولة والشركات التابعة لها القيام بجميع الإجراءات اللازمة للحفاظ على امن المعلومات الخاصة بها(47-31 من قانون الجرائم الإلكترونية وجرائم تكنولوجيا الاتصالات والمعلومات)

وفي المادة 48 إعادة المشرع تنظيم الأحكام الخاصة بالعقوبات المقررة للاشتراك في ارتكاب إحدى الجرائم المنصوص عليها في قانون الجرائم الإلكترونية حيث نص على عقوبة من يشترك بالاتفاق والتحريض أو المساعدة والتدخل في ارتكاب جناية أو جنحة بنفس العقوبة المقررة للفاعل الأصلي وفي حال عدم وقوع الجريمة يعاقب بنصف العقوبة

ويلاحظ من خلال النص المذكور أعلاه أن المشرع كرر فيه الحكم المنصوص عليه في المادة (28) من نفس القانون مع الأخذ بعين الاعتبار إضافة العقوبة المقررة في حالة عدم وقوع الجريمة محل التحريض والاتفاق، وهنا يمكن القول أن على المشرع وتجنبا للتكرار الوارد في هذه المواد الاكتفاء بنص المادة 48 كونها أشمل في الحكم ويكفي لمعالج الحالة المذكور في المادة 28 وعليه نقترح على المشرع إجراء تعديل يتضمن إلغاء نص المادة 28.

هذا وقد نظم المشرع في هذا القانون الأحكام الخاصة بالعقوبة المقررة على الشروع في هذه الجرائم وكذلك العقوبات التكميلية التي تستطيع المحكمة النطق بها على مرتكبي هذه الجرائم. كما نص المشرع على مجموعة الظروف التي تشدد العقوبات المفروضة على هذه الجرائم. والحالات التي يتم فيها إعفاء الجناة من العقوبة المقررة على هذه الجرائم وكذلك شروط الاستفادة منها. (49، 53،52،51،50)

ويلاحظ من خلال استقراء وتحليل بعض النصوص الواردة في قانون الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات أن المشرع الفلسطيني نص على نسبة كبيرة من أحكام الجرائم الإلكترونية خاصة تلك المتعلقة بالأحكام الموضوعية، وكذلك العديد من الأحكام الإجرائية المتعلقة بملاحقة مرتكبي هذه الجرائم، كما أن

المشرع وبالرغم من قيامه بتعديل هذا القانون أكثر من مرة، إلا أن هذا التعديل لم يأتي على مسألة هيكل هذا القانون، حيث بقيت الأحكام الموضوعية والإجرائية الواردة فيه على حالها، دون أي تصنيف أو تنظيم خاص بتوبيها أو عناوينها

وانطلاقاً مما سلف، يمكننا إجمال أوجه القصور في قانون الجرائم الإلكترونية الفلسطيني التي تم ملاحظتها في تنظيم ومعالجة بعض أحكام هذه الجرائم، والتي ظهرت في مواضع كثيرة من هذا القانون، ولعل من أبرزها عدم اتباعه منهجاً معيناً في تصنيف وتنظيم هذه الجرائم، حيث جاء هذا القانون خالياً من أي تصنيف أو مسمى لهذه الجرائم، حيث تم النص على أحكامها بشكل غير دقيق و ظهر هذا القصور جليا في النواحي التالية:

1. من الناحية الموضوعية لم ينظم المشرع الجرائم في هذا القانون وفق معيار محدد، خاصة من حيث وجودها ضمن مجموعات أو فئات تجمع بينها عناصر مشتركة أو بناءً على طبيعة الحق المعتدى عليه

2. لم يضع المشرع مسمى أو عناوين لهذه الجرائم يسهل على أصحاب الاختصاص والمهتمين التعامل مع النصوص الوارد في هذا القانون

3. بالرغم من أن هذا القانون وضع لتنظيم أحكام الجرائم الإلكترونية، إلا أن هناك بعض النصوص جاءت فيه لتنظم بعض الحقوق المتعلقة بحرية الرأي والتعبير وإنشاء الصحف والمواقع الإلكترونية وغيرها من وسائل التعبير، دون أن يقترن انتهاك هذه الحقوق بعقوبة، فكل ما تضمنته مجرد حث السلطات المختصة على احترام هذا الحق، حيث اعتبر المشرع أن جميع الأفعال التي يتضمنها هذا الحق تعتبر مبررة ولا يجوز مصادرة وسائل التعبير المختلفة ألا بأمر قضائي أو إيقاع أي عقوبة سالبة للحرية أو التوقيف بسبب القيام بالتعبير عن الرأي، لكن في المقابل لم يفرض المشرع أي جزاء على مخالفة هذا النص.(المادة 21 من قانون الجرائم الإلكترونية الفلسطيني )

ويرى الباحث عدم وجود مبرر وضرورة لوجود هذا النص ضمن قانون الجرائم الإلكترونية، نظرا لخصوصية هذا القانون المتعلقة بالتجريم والعقاب و إجراءات الملاحقة، بالإضافة إلى أن هذا الحقوق كفلها المشرع في القانون الأساسي الفلسطيني ونظم أحكام بشكل مفصل بموجب أحكام القانون رقم (9) لسنة 1995 بشأن المطبوعات والنشر، وأن كان لابد من وجود هذا النص ضمن قانون الجرائم الإلكترونية فحري على المشرع وضعه ضمن الشق الإجرائي في هذا القانون في حال تم تعديله مستقبلا وتجزئته لأحكام موضوعية وأخرى إجرائية

4. هناك مسألة أخرى وهي مرتبطة بوجود بعض الأحكام المكررة في هذا القانون خاصة تلك المتعلقة بالعقوبات المفروضة على الاشتراك الجرمي عن طريق التحريض أو الاتفاق أو المساعدة أو التدخل، حيث كرر المشرع حكم هذه الأفعال في المادة (48، 28) علما أن هذه النصوص يمكن دمجها في نص واحد كونها تحتوي على نفس الأحكام بالنسبة للعقوبة

5. بالإضافة إلى ذلك أن المشرع لم ينص على جميع الأحكام الخاصة بالظروف بالإعفاء والتخفيف والتشديد على المشددة العقوبات المقررة للجريمة

6. لم يقم المشرع الفلسطيني بالفصل في هذا القانون بين الأحكام الموضوعية والإجرائية التي تختلف بموضوعها، حيث نص على إجراءات ملاحقة مرتكبي هذه الجرائم بشكل غير منتظم في مواضع مختلفة في جميع أجزائه الأمر الذي يتطلب إدراجها في القانون وفق تسلل وتنظيم معين

## الفرع الثاني: تنظيم وتصنيف الجرائم الإلكترونية في التشريع الإماراتي

لقد كانت دولة الإمارات العربية المتحدة من أوائل الدول على المستوى العربي في المبادرة إلى سن تشريع خاص لمكافحة الجرائم الإلكترونية، حيث أصدر المشرع في العام 2006 القانون رقم ( 2) في شأن مكافحة الجرائم الإلكترونية وقد تضمن القانون التعريف بالمعلومات الإلكترونية والبرنامج المعلوماتي ونظام المعلومات الإلكتروني والشبكة المعلوماتية والمستند الإلكتروني للموقع الإلكتروني ووسيلة تقنية المعلومات والبيانات الحكومية.(المختن، 2015 ص43)

بالإضافة إلى ما سبق فالمشرع الإماراتي ولمواكبة التطور الحاصل في مواجهة ظاهرة الإجرام الإلكتروني، قام بإجراء العديد من التعديلات تمثلت بإصدار المشرع الإماراتي القانون الاتحادي رقم (5) لسنة 2012 م في شأن مكافحة الجرائم الإلكترونية. والذي عدل بموجبه القانون رقم (2) في شأن مكافحة الجرائم الإلكترونية لسنة 2006.

ولعل من أهم ما جاء به هذا القانون من تعديلات، وضع المشرع تعريفات للمصطلحات الواردة في القانون التي من شأنها أن تساهم في توضيح بعض المصطلحات التقنية، التي قد تشكل صعوبة في فهم هذه الجرائم كونها من مصطلحات مرتبطة بالتقنيات الحديثة التي لم يعهد المشرع التعامل معها في اللغة القانونية (عمر،2019،ص715)

كما تميز هذا القانون بقيام المشرع الإماراتي بإجراء العديد من التعديلات الأخرى والتي ساهمت بدورها في وضع سياسة جنائية متطورة تنسجم مع متطلبات مواجهة هذه الجرائم على المستوى التشريعي، لاسيما تلك المتعلقة بتجريم بعض الأفعال والتشدد في العقوبات المفروضة على بعض الجرائم وكذلك الأخذ بالتدابير الاحترازية وحالات الإعفاء والتخفيف في حالة الإبلاغ عن الجرائم المنصوص عليها بهذا القانون وغيرها من التعديلات التي هدف المشرع من ورائها تحقيق الأمن الإلكتروني بأبعاده المختلفة(المختن،2015،ص46 وبعدها)

ومما لا شك فيه أن المشرع الإماراتي خطى خطوة متقدمة في تنظيمه للأحكام المتعلقة بالجرائم الإلكترونية، تمثلت بإصدار القانون الاتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية الذي حل محل القانون رقم 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

ويرى بعض الخبراء أن التعديل الذي أجراه المشرع الإماراتي على قانون مكافحة الجرائم الإلكترونية، جاء ليعبر عن رغبة المشرع في وضع تنظيم أكثر فعالية لاستعمال الإنترنت ومكافحة الجرائم الإلكترونية، حيث يعتبر هذا القانون من أحدث التشريعات وأكثرها تطورا، من حيث تناوله المجالات الأكثر أهمية، و أي نشاط في الفضاء السيبراني الذي يشكل تهديداً للدولة، ويشكل مخالفة للنظام العام والآداب فيها )الصفر للمحاماة والاستشارات القانونية 2022)

فالمشرع الإماراتي من خلال إصداره لقانون مكافحة الشائعات والجرائم الإلكترونية خطى خطوة متطورة على المستوى العربي، لاسيما في تنظيمه للأحكام الموضوعية والإجرائية المرتبطة بالجرائم الإلكترونية، حيث نظم في هذا القانون جزء كبير من المسائل المرتبطة في مكافحة ظاهر الإجرام الإلكتروني، فقد جاء هذا القانون ليعالج الأحكام الخاصة بهذه الجرائم بما يتماشى مع التطورات التي تحدث في قطاع التكنولوجيا، بالإضافة إلى مسألة تنظيمه الأحكام المختلفة بشكل منهجي في إطار هذا القانون.

ولعل من أبرز ملامح السياسة الجنائية التي اتباعها المشرع الإماراتي في تنظيم أحكام الجرائم الإلكترونية في هذا القانون، هو الفصل بين الأحكام الموضوعية والإجرائية الخاصة بملاحقة مرتكبي هذا النوع من الجرائم، حيث قسم المشرع هذا القانون إلى بابين في الأول نظم الأحكام الموضوعية، وفي الثاني حدد فيه الأحكام الإجرائية المتعلقة بملاحقة مرتكبي هذه الجرائم، ويتميز هذا القانون تصنيفه وتبويبه الجرائم الإلكترونية ضمن هذا القانون

ضمن مجموعات، كما تميز هذا القانون في وضع تعريف للمصطلحات الواردة في هذا القانون وهي المصطلحات التي يغلب عليها طابع التخصص في مجال تكنولوجيا المعلومات، حيث عرف المشرع في المادة (1) من قانون مكافحة الشائعات والجرائم الإلكترونية المصطلحات العلمية اللازمة لتطبيق أحكام هذا القانون تضمنت هذه المادة غالبية المصطلحات التي تفيد في فهم وتطبيق هذا القانون

كما يتميز هذا القانون بوضعه عناوين ومسميات للجرائم،حيث يشكل هذا الأمر مسألة حيوية على صعيد فهم وتحليل هذه الجرائم وصولا إلى تكيفها، فهذه الجرائم ترتبط بشكل أو بأخر وبغض النظر عن تصنيفها ترتبط في مجال التكنولوجيا حيث تستخدم المسميات والمصطلحات ذات الطابع التقني الذي قد يثير بعض الاختلاف على المختصين لتميز هذه الجرائم

وللوقوف على تفاصيل منهج المشرع سنتناول في هذا الجزء من البحث تنظيم المشرع الإماراتي الأحكام الجرائم الإلكترونية على النحو الآتي:

## أولا: بالنسبة لمعالجة للأحكام الموضوعية الخاصة بالجرائم الإلكترونية:

قسم المشرع الإماراتي الباب الخاص في الأحكام الموضوعية للجرائم الإلكترونية إلى ثلاث فصول حيث جمع في الفصل الأول والثاني مجموعة من الجرائم التي تشترك جميعها في محل الجريمة الذي تربطه خصائص وعناصر مشتركة، كما خصص المشرع الفصل الثالث للعقوبات والتدابير الخاصة بهذه الجرائم

في الفصل الأول من هذا الباب والذي جاء تحت عنوان الجرائم الواقعة على تقنية المعلومات نظم المشرع أحكام جميع الجرائم التي يكون محل الاعتداء فيها تقنية المعلومات بمفهومها الواسع، حيث تضمن هذا الفصل في مواده المختلفة جميع الجرائم التي تمس تقنية المعلومات في كافة أشكالها وأنواعها فجرم الاختراق الإلكتروني بمختلف صوره سواء كان اختراق أنظمة المعلومات الخاصة بالأفراد أو المؤسسات أو اختراق أنظمة المعلومات التابعة للدولة.(المواد2، 3،)من قانون مكافحة الشائعات الجرائم الإلكترونية الإماراتي.[2]

كما جرم المشرع في هذا الفصل كل فعل يرتكب عمدا من شأنه إلحاق الضرر في المعلومات وأنظمة تقنية المعلومات وسائلها التي تعود للأفراد أو المؤسسات أو تلك التي تعود لإحدى مؤسسات الدولة أو مرافقها الحيوية، سواء تم ذلك بإتلافها أو التلاعب بها أو تحريفها أو إيقاف أو تعطيل الأنظمة والشبكات.وحدد المشرع ضمن هذه النصوص الظروف المشددة التي قد تقترن بها هذه الأفعال

وفي السياق ذاته أورد المشرع الإماراتي الجرائم التي يكون محلها البيانات الخاصة بالأفراد والدولة أو مؤسساتها وكذلك البيانات الخاصة بالمنشآت التجارية والمالية والاقتصادي، حيث نص على تجريم جميع الأفعال التي تقع على البيانات التابعة لهذه الجهات سواء كان ذلك بإتلافها أو حذفها أو الحصول أو نسخها عليها أو إفشائها بشكل غير مشروع، كما الحق المشرع بموجب هذه النصوص الظروف التي من شأنها تشديد العقوبة على هذه الأفعال. المواد (6، 7، 8 قانون مكافحة الشائعات و الجرائم الإلكترونية)

2 في هذه البحث أينما تم الإشارة لقانون مكافحة الشائعات و الجرائم الإلكترونية الإماراتي، يقصد به المرسوم بقانون رقم 34 بشأن مكافحة الشائعات والجرائم الإلكترونية
وحرصا على عدم تكرار ذكر اسم القانون فإن جميع النصوص الوارد في الفرع الثاني من المطلب الثاني مصدرها التشريع الإماراتي المذكور أعلاه.)

كما فرض المشرع الإماراتي عقوبات على كل من يتحايل على العنوان الإلكتروني للشبكة الإلكترونية وذلك باستخدام معلومات أو عناوين تخص الغير أو بأي وسيلة كانت بقصد ارتكاب جريمة أو منع اكتشافها، وكذلك جرم اصطناع البريد أو الموقع أو الحساب الإلكتروني المزيف وشدد العقوبة على هذه الأفعال حال تم استخدام الموقع لأمر مسيء لصاحب الموقع المصطنع أو كان الاصطناع يعود لمواقع رسمية للدولة (المواد 10، 11)

هذا وقد خصص المشرع أحكام المواد(12، 13، 14،15) من هذا القانون لتجريم اعتراض المعلومات أو إعاقة الوصول إليها بطريقة غير مشروعة وكذلك إفشاء المعلومات المعترضة، وشدد العقوبة في حال كانت المعلومات أو البيانات المعترضة تعود للدولة وكذلك جرم تزوير واستعمال المستندات الإلكترونية، والاعتداء على وسائل الدفع الإلكترونية.

كما جرم المشرع استخدام المواقع الإلكترونية لارتكاب الجرائم وكذلك إخفاء الأدلة المتحصلة منها كذلك إنشاء وإدارة المواقع الإلكترونية بقصد ارتكاب جريمة أو تسهيل ارتكابها، بالإضافة إلى تجريم قيام المسؤول عن إدارة الموقع أو الحساب أو البريد الإلكتروني أو نظام الكرتوني بإخفاء أو العبث في الأدلة المتعلقة بارتكاب احدى الجرائم المنصوص عليها في هذا القانون بهدف إعاقة عمل السلطات المختصة بالتحريات والتحقيق بها.(16 ،17، 18 من قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي )

وفي نهاية الفصل الأول من هذا الباب أورد المشرع نص خاصا جرم فيه قيام أي مسؤول عن أدارة موقع أو حساب الكرتوني يقوم بنشر معلومات أو محتوى أو بيانات لا تتوافق مع معايير المحتوى الإعلامي الصادر عن الجهات ذات العلاقة

وبهذا الصدد يرى الباحث والنظر إلى الأفعال التي التي يتكون منها السلوك الإجرامي في النص المذكور أعلاه، والمتمثلة بنشر معلومات أو محتوى لا يتفق مع المعايير التي وضعتها السلطات المعنية للنشر، أقرب إلى جرائم المحتوى منه إلى الجرائم الواقعة تقنية المعلومات

وعلاوة على ذلك أن المشرع الإماراتي أورد في الفصل الثاني من الباب الأول من هذا القانون والذي جاء تحت عنوان جرائم المحتوى ونشر الشائعات حيث خصصه هذا الفصل لتنظيم كل ما يتعلق تجريم الأنشطة الإجرامية التي تمس سلامة المحتوى الذي يتم تداوله على المواقع الإلكترونية وكذلك أنظمة المعلومات والشبكات، فقسم المشرع هذا الفصل إلى فرعين في الأول حدد المشرع الجرائم التي تمس سلامة المحتوى، وفي الثاني نص على تجريم نشر الشائعات والأخبار الزائفة.

وتأسيساً على ذلك؛ ولغاية حسن الصياغة والدقة في تصنيف وتنظيم أحكام هذه الجرائم في قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي يقترح الباحث وضع هذا النص إطار الفصل الثاني من الباب الأول والذي تضمن جرائم المحتوى

وبالرجوع إلى الأحكام الواردة في الفرع الأول من الفصل الثاني، نجد أن المشرع قام بالنص على تجريم مختلف صور وأشكال المساس بسلامة المحتوى، فجرم الدعوة والترويج التي تهدف إلى تعطيل أحكام الدستور والقانون، والتجنيد والترويج للجماعات الإرهابية أو المنظمات والمجموعة غير المشروعة، وكذلك نشر المعلومات التي تلحق الضرر بمصالح الدولة.(20،21،22 قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي )

وفي المادة (23) من نفس القانون نص المشرع على تجريم التحريض على المساس بأمن الدولة والاعتداء على مأموري الضبط القضائي، حيث جرم المشرع في هذا النص القيام بإنشاء أو إدارة موقع إلكتروني أو الإشراف عليه أو استخدام أي من وسائل تقنية المعلومات بقصد التحريض أو القيام بأفعال نشر معلومات أو رموز أو صور أو رسوم أو غيرها وكان من شأنها تعريض أمن الدولة ومصالحها العليا للخطر والمساس والنظام العام فيها أو الاعتداء المكلفين في إنفاذ هذا القانون

نلاحظ من خلال تحليل هذا النص أن المشرع جمع في نص واحد تجريم أفعال يكون فيها محل الاعتداء مختلف فمن ناحية جرم القيام بالأفعال المذكور في النص حيث يكون فيها محل الاعتداء أمن الدولة ومصالحها العليا ونظامها العام، ومن ناحية أخرى جرم القيام بنفس الأفعال عندما يكون هدفها الاعتداء على المكلفين بملاحقة مرتكبي الجرائم وإنفاذ القوانين. وهي جرائم بطبيعتها تشكل موضوعات مختلفة فالجرائم التي تقع الأشخاص المكلفين بإنفاذ القانون تدخل ضمن إطار الجرائم الواقعة على السلطات العامة في الدولة مع الأخذ بعين الاعتبار اختلاف وصفها القانوني بناء على النتيجة فالمشرع قد يعتبر في بعض الأحيان الاعتداء على موظف عام ظرف مشدد كما هو الحال في جرائم القتل والإيذاء وقد يعتبر جريمة عندما يقع في إطار إعمال الشدة ومقاومة الموظفين والاعتداء عليه بأي فعل قد ينتج عنه المساس بسلامتهم.

وبناءً عليه ومن تحليل النص المذكور أعلاه ونظرا لاختلاف طبيعة الحق المعتدى عليه في هذا النص ومن أجل دقة التصنيف وحسن الصياغة يرى الباحث الفصل ما بين الأفعال المذكورة فيه في نصوص مستقلة

ومن الأفعال التي جرمها المشرع الإماراتي بموجب أحكام الفصل الثاني، إنشاء وإدارة المواقع الإلكترونية أو الأشراف عليها بغرض القيام بالترويج لإثارة الفتنة والإضرار بالوحدة الوطنية ونشر الأفكار أو معلومات تتضمن أثارة الفتنة أو العنصرية أو التجنيد لها، وكان من شأن هذه الأفعال الإضرار بالسلم الأهلي والإخلال بالنظام العام والآداب العامة في الدولة. وفرض عقوبة على كل من يقوم بإحدى الوسائل المذكورة السخرية والإضرار بسمعة الدولة ورموزها الوطنية والترويج والدعوة للقيام بمظاهرات دون الحصول على الإذن المسبق، التحريض على عدم الالتزام بالقوانين المعمول بها في الدولة ونشر معلومات من شأنها الإساءة لدولة أجنبية(المواد 24، 25، 26، 27، 28)

وفي هذا الإطار وضمن الفصل الثاني نص المشرع على تجريم استخدام شبكة معلوماتية أو واحدى تقنية المعلومات للإتجار والترويج للأسلحة أو الذخائر والمتفجرات، وكذلك استخدام هذه الوسائل لغسل الأموال والإتجار بالمخدرات أو الترويج لها والإتجار بالبشر والتحريض على الفجور و الدعارة ونشر المواد الإباحية والمساس بالآداب العامة واستخدام الأطفال في إعداد المواد الإباحية وحيازة مواد إباحية للأطفال

كما خصص المشرع جزء من نصوص هذا الفصل لمعاقبة كل من يرتكب بواسطة الشبكة المعلوماتية أو احدى وسائل تقنية المعلومات أو الموقع الإلكترونية الإساءة للدين والمقدسات الإسلامية وكذلك الإساءة للأديان الأخرى والترويج للعب القمار والإتجار غير المشروع بالآثار والتحف والاحتيال الإلكتروني والحصول على الأموال بطريقة غير مشروعة

ومن الأفعال التي حرص المشرع على تجريمها في هذا الفصل، استخدام وسائل تكنولوجيا المعلومات لارتكاب التهديد والابتزاز الإلكتروني والقيام بالسب والقذف والاعتداء على خصوصية وحرمة الحياة الخاصة في غير الأحوال المصرح بها قانونا، وكشف المعلومات السرية المرتبطة بالعمل أو المهنة، والدعوة والترويج لجمع تبرعات مالية دون الحصول إجراء الاستطلاعات والمسوحات الاجتماعية على الإذن المسبق من السلطة المختصة في الدولة ( 42، 43، 44، 45، 46، 47)

كما أدرج المشرع في إطار هذا القانون الإعلان والترويج التي تقع بغرض تضليل المستهلك وكذلك الترويج للمنتجات الطبية والعلاجية المقلدة، والاستفادة من الخدمات التي تقدمها شركات الاتصال والبث دون حق، والتسول الإلكترونية (48 ،49، 50، 51، 52)

وأما بالنسبة للفرع الثاني من هذا الفصل والذي جاء تحت عنوان جرائم النشر والشائعات فقد خصصه المشرع لتجريم نشر الشائعات والأخبار الكاذبة وإتاحة المحتوى غير قانوني وعدم إزالته، وإنشاء أو تعديل ربوتاتات زائفة لنقل بيانات أو معلومات زائفة داخل الدولة، والحصول على مقابل لنشر محتوى غير قانوني

وفي الفصل الثالث من هذا الباب تناول المشرع الإماراتي الأحكام الخاص بالعقوبات والتدابير الاحترازية التي يمكن أن يتوقع على مرتكب واحدة من الجرائم المنصوص عليها في هذا القانون حيث تضمن هذا الفصل النص على المصادرة وكذلك على العقاب على الشروع في جميع الجنح المنصوص عليها، وكذلك حدد مسؤولية المدير الفعلي للشخص الاعتباري عن الجرائم الإلكترونية التي ترتكب وكان عالما بها، وكذلك مسؤوليته عن التعويض عن الأضرار التي تقع بسبب ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون، كما حدد المشرع في هذا الفصل حالات التشديد والإعفاء والتخفيف من العقوبة المقرر في هذا القانون

مما سبق نلاحظ أن المشرع الإماراتي خرج عن القواعد العامة بالنسبة للعقاب على الشروع في ارتكاب الجنح حيث عاقب بموجب أحكام المادة(57) على الشروع على ارتكاب جميع الجرائم الجنحية المنصوص عليها في هذا القانون. وساوى كذلك بالمسؤولية المترتبة على ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون، بين المدير الفعلي للشخص الاعتباري وفاعل الجريمة في حال ارتكبت الجريمة وثبت علمه بها

كما أجاز المشرع بموجب أحكام هذا القانون للجهات المختصة إصدار أوامر التعطيل والتصحيح والإيقاف وكذلك حظر الوصول إلى المواقع والشبكات التي يثبت تداولها ونشرها لمعلومات وبيانات زائفة أو محتوى غير مشروع، كما أجاز المشرع للمتضرر من هذه الأوامر الطعن والتظلم على هذه القرارات أمام المرجعيات القضائية المختصة وفق الإجراءات المنصوص عليها في هذا القانون(62،63)

ونظم المشرع في نهاية الباب الأول حالات عدم انتفاء المسؤولية عن ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون، حيث نص على ذلك صراحة في المادة(64)

وفي الباب الثاني من هذه القانون الذي جاء تحت عنوان أحكام إجرائية وختامية تناول المشرع الأحكام المتعلقة بإجراءات ملاحقة مرتكبي هذه الجرائم والجهات المختصة بها وكذلك الأحكام الخاصة بحجية الأدلة التي يجوز قبولها لإثبات هذه الجرائم، كما نظم الأحكام الخاصة بالتصالح في هذه الجرائم وكذلك الأحكام الخاصة بالنطاق المكاني لسريان هذا القانون

كما حدد المشرع بموجب أحكام هذا القانون الجهات الممنوحة صفة مأموري الضبط في ملاحقة مرتكبي الجرائم المنصوص عليها في هذا القانون وإثباتها، والجرائم التي تعتبر بموجب أحكام هذا القانون من الجرائم الماسة بأمن الدولة

وبعد أن انتهينا من استقراء خطة المشرع الإماراتي في تصنيف وتنظيم الأحكام الخاصة بالجرائم الإلكترونية وبعد تحليل موجز لبعض النصوص الواردة في قانون مكافحة الشائعات والجرائم الإلكترونية نلاحظ ما يلي:

1. أن المشرع الإماراتي اعتمد في تنظيمه وتبويبه لهذا القانون على قاعدة الفصل ما بين الأحكام الموضوعية والإجرائية
2. حصر المشرع الإماراتي أحكام معظم الأفعال التي قد ترتكب باستخدام الشبكات التقنيات الحديثة.
3. اعتمد المشرع في تصنيفه للجرائم وتبويبه للأحكام الموضوعية في قانون الجرائم إلى على أساس طبيعة الحق المعتدى عليه أو المصلحة المحمية
4. حصر المشرع الوسائل الخاصة بارتكاب هذه والتي قد ترتكب بها هذه الجرائم وهي وسائل تعتمد في أساسها على استخدام التكنولوجيا والشبكات والمواقع الإلكترونية أو إدارتها أو إنشائها. وهذا بدوره يساهم في التمييز بين هذه الجرائم والجرائم الأخرى التي ترتكب بوسائل تقليدية

## الخاتمة:

تعد مسألة تصنيف الجرائم في إطار القانون الجنائي بشكل عام من المسائل الهامة، تظهر في جميع مراحل المعالجة القانونية لمكافحة الجريمة، كما أن لهذا التصنيف أهمية خاصة في موضوع مكافحة الجرائم الإلكترونية، هذا النوع الحديث من الأجرام القابل بطبيعته للتطور المستمر؛ وذلك بسبب ارتباطه بالتطور الحاصل في مجال استخدام التقنيات الحديثة في حياة الإنسان. وبعد أن تناولنا في هذا التصنيفات المختلفة للجرائم الإلكترونية وخصوصية الحق المعتدى عليه وأهميته في تصنيفها، وكذلك بعد إجراء مقارنة لتنظيم هذه الجرائم وتصنيفها وتبويبها في القانون الفلسطيني والإماراتي، توصلنا إلى مجموعة من النتائج والتوصيات نجملها على النحو الآتي:

## النتائج:

1. أن تصنيف الجرائم الإلكترونية وفق معيار طبيعة الحق المعتدى عليه له أهمية على المستوى التشريعي، تكمن في تسهيل إجراء التعديلات المتعلقة بتجريم الأفعال التي قد تظهر مستقبلا، والتي قد تنجم عن تطور وسائل ارتكابها، بالإضافة إلى أهميته في مراحل عملية الملاحقة لمرتكبي هذه الجرائم لاسيما في موضوع التكييف القانوني لها

2. بالرغم من أهمية خطوة المشرع الفلسطيني في إصدار تشريع خاص لمكافحة الجرائم الإلكترونية وإجراء العديد من التعديلات عليه، الأن هذا القانون لازال بحاجة إلى بعض التعديلات لاسيما تلك المتعلقة بتصنيف وتبويب الجرائم فيه.

3. يشكل تصنيف الجرائم الإلكترونية حسب طبيعة الحق المعتدى عليه التصنيف الأهم لما له من دور أساسي في فهم حقيقة هذه الجرائم والوقاية منها ومكافحتها

4. أن وضع مسمى أو عناوين للجرائم يسهل على أصحاب الاختصاص والمهتمين التعامل مع النصوص الوارد في قانون الجرائم الإلكترونية

5. يمثل قيام المشرع الإماراتي بإجراء التعديلات على القانون الخاص بمكافحة الشائعات و الجرائم الإلكترونية مسألة هامة تنسجم مع متطلبات مواكبة التطور الحاصل في مجال ظاهر الإجرام الإلكترونية، بشكل يسهل عملية استيعاب أي نوع جديد من هذه الجرائم

## التوصيات:

1. ضرورة قيام المشرع الفلسطيني بإجراء تعديل على تنظيم الجرائم في قانون الجرائم الإلكترونية بشكل ينسجم وطبيعة هذه الجرائم والأخذ بمعيار طبيعة الحق المعتدى عليه لهذه الغاية

2. العمل على الفصل بين الأحكام الإجرائية والموضوعية في قانون الجرائم الإلكترونية من خلال تقسيم هذا القانون إلى جزئين، جزء ينظم الأحكام الموضوعية وأخر يتضمن الأحكام الإجرائية

3. العمل على تبويب و وضع مسميات وعناوين للجرائم الوارد في قانون الجرائم الإلكترونية الفلسطيني.

4. إجراء تعديل لبعض النصوص الواردة في قانون الجرائم الإلكترونية الفلسطيني، خاصة تلك المتعلقة بتنظيم بعض الأحكام الموضوعية لاسيما الحكم المنصوص عليه في المادة (28) مع الأخذ بعين الاعتبار إضافة العقوبة المقررة في حالة عدم وقوع الجريمة محل التحريض والاتفاق

5.نقترح على المشرع الفلسطيني إلغاء نص المادة (28)وذلك تجنبا لتكرار الأحكام الوارد فيها المادة (28) والاكتفاء بنص المادة 48 كونه اشمل لتنظيم الأحكام التي قصدها المشرع لعلاج الحالات المذكورة

6. تعديل نص المادة 21 من قانون الجرائم الإلكترونية الفلسطيني بحيث يتم إلغاء الفقرة الأولى والثالثة من هذه المادة بحيث تقتصر على إجراءات الملاحقة والمصادرة بالإضافة إلى ضرورة النص على الجزاءات التي قد تترتب على الإخلال بشروط الملاحقة، وعليه نقترح التعديل التالي:

أ. لا يجوز رفع أو تحريك الدعاوى لوقف أو مصادرة الأعمال الفنية والأدبية والفكرية أو ضد مبدعيها إلا بأمر قضائي صادر عن المحكمة المختصة، ولا توقع عقوبة سالبة للحرية أو التوقيف الاحتياطي في الجرائم التي ترتكب بسبب علانية المنتج الفني أو الأدبي أو الفكري لا يجوز فرض قيود على الصحافة أو مصادرتها أو وقفها أو إنذارها أو إلغاؤها إلا وفقاً للقانون، وبموجب حكم قضائي

ب. صادر عن المحكمة المختصة

ج. يترتب البطلان على مخالفة أي حكم من الأحكام الواردة في الفقرتين (1،2) من هذه المادة.

## قائمة المصادر والمراجع:

- **القوانين والاتفاقيات الدولية:**


- التقرير التفسيري لاتفاقية الجرائم الإلكترونية بودابست( 2001)، مجلس أوروبا
- البروتوكول الملحق باتفاقية بودابست( 2002 )، مجلس أوروبا
- قرار بقانون رقم ( 10) لسنة 2018 م بشأن الجرائم الإلكترونية وجرائم الاتصالات وتكنولوجيا المعلومات وتعديلاته
- قانون الإجراءات الجزائية الفلسطيني رقم(3) لسنة 2001 م
- مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية


- **الكتب القانونية:**


- المردني، محمود(2022). النظام القانوني للجريمة الإلكترونية والمعلوماتية، دار العلم والإيمان للنشر والتوزيع.
- الخن، طارق(2018). جرائم المعلومات، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية.
- ابراهيم،خالد (2009).جرائم المعلومات، الإسكندرية: دار الفكر الجامعية
- الحسيناوي، علي( 2009 ).جرائم الحاسوب والإنترنت، عمان :دار اليازوري العلمية للنشر والتوزيع.
- الحجار حلمي، والحجار راني (0201).المنهجية في حل النزاعات ووضع الدراسات القانونية،ط1،منشورات الحلبي الحقوقية، بيروت، لبنان.
- السراج،عبود(2018). قانون العقوبات العام ج1، منشورات الجامعة السورية الافتراضية،سوريا
- الجنبيهي، ممدوح،(2006 ).جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها الإسكندرية :دار الفكر الجامعي.
- الفاضل، محمد(1962).الجرائم الواقعة على الأشخاص، الطبعة الثانية، إصدار جامعة دمشق.
- باطلي، غنية (2015). الجريمة الإلكترونية، دراسة مقارنة منشورات الدار الجزائرية : الجزائر
- توبة عبد الحكيم(2009 ).جرائم تكنولوجيا المعلومات ط1 عمان، دار المستقبل للنشر والتوزيع
- عبيد، عماد (2018). قانون العقوبات الخاص ج.2، منشورات الجامعة السورية الافتراضية، سوريا
- فرج، يوسف(2008 )،الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية، الاسكندرية
- نصار،غادة (2017).الإرهاب والجريمة الإلكترونية ، القاهرة : العربي للنشر والتوزيع.

- **الأبحاث العلمية :**

- أسمهان، بن مالك(2019). خصائص الجريمة المعلوماتية وأسباب ارتكابها، مجلة البيان للدراسات القانونية والسياسية، عدد 4 ص 124-102
- المختن، عبيد صالح(2015). سياسة المشرع الإماراتي لمواجهة الجرائم الإلكترونية. مجلة الفكر الشرطي، مج. 24، ع. 4، ص ص.52-21.
- الغافري، حسين، (2007).دراسة في الجهود الدولية في مواجهة جرائم الإنترنت، من منشورات المنشاوي للدراسات والبحوث.
- الصفر للمحاماة والاستشارات القانونية(2022). مكافحة الجرائم الإلكترونية، مقال منشور على موقع *https://ae.linkedin.com*
- سميرة، معاشي (2018). الجريمة المعلوماتية «دراسة تحليلية لمفهوم الجريمة المعلوماتية»، مجلة دار الفكر، العدد 17، ص 417-398
- عمر، بن ياسين (2019). المعالجة القانونية للجرائم الإلكترونية في التشريع الجزائري والتشريعات المقارنة(التشريع المغربي والإماراتي أنموذجا)، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 3، ص ص 227-710.
- علكوم، وليد،( 2000). مفهوم ظاهرة الإجرام المعلوماتي، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت-جامعة الإمارات
- عرب، يونس.( 2002). جرائم الكمبيوتر والإنترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، تنظيم المركز العربي للدراسات والبحوث الجنائية
- فتيح رعد، وعواد ياسر، (2017). إثبات الجريمة الإلكترونية بالدليل العلمي،مجلة جامعة تكريت للحقوق، العدد 3، الجزء 2
- معهد الدراسات السياسية والاقتصادية الفلسطيني(2012). دراسة نقدية للإطار القانوني للجرائم الإلكترونية في الأراضي الفلسطينية.
- محمد عبد الرحيم (2015). دراسة الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها،استرجعت من موقع *2019/1/http://dr-ama.com/wp-content/uploads*

- **الرسائل الجامعية:**

- العجمي، دغمش(2014).المشاكل العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة ماجستير، من منشورات جامعة الشرق الأوسط.
- البتاتي محمد(2002). المصلحة المحمية بالتجريم، أطروحة دكتوراه، كلية القانون، جامعة الموصل
- أبو جامع، أسامة (2016). تكييف الواقعة الإجرامية في القانون الجزائي الفلسطيني «دراسة تحليلية»، رسالة ماجستير، من منشورات كلية الحقوق جامعة الأزهر، غزة، فلسطين
- صالح بن منصور، وأنيسة كوش(2015). السلوك الإجرامي للمجرم المعلوماتي، رسالة ماجستير، جامعة عبد الرحمان ميرة، الجزائر.

المراجع الأجنبية:

- Raghavan ,A. & Parthiban, L. (2014).The growing Case Of Cybercrime & Type's Of Cybercrime On Global Scale , *A Journal of Computer Science Engineering and Information Technology Research Vol. 4, Issue 2, p, 1-6*

- Jahankhani , H. , Al-Nemrat, A., & Hosseinian, A.,(2014) *Cybercrime classification and characteristics . https://www.researchgate.net*

- *The Global Risks Report 2023 18th Edition Insight Report*

*https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf*

- United Nations Office on Drugs and Crime(2015) *International Classification Of Crime For Statistical Purposes (ICCS) Version 1*

## List of sources and references in English:

- **rules and Conventions**

- Interpretative Report of the Budapest Convention on Cybercrime (2001). Council of Europe
- Protocol to the Budapest Convention (2002). Council of Europe
- Decree-Law No. (10) of 2018 regarding electronic crimes and its amendments
- The Palestinian Criminal Procedures Law No. (3) of 2001 AD
- Federal Decree-Law No. (34) of 2021 regarding combating rumors and elecotonic crime

- **Legal books**

- Al-Mardani, Mahmoud (2022). *The legal system of cyber and informatics crime*, Dar Al-Ilm and Al-Iman for publication and distribution.

- Al-Khan, Tariq (2018). *Information Crimes,* Syrian Virtual University Publications, Syrian Arab Republic.

- Ibrahim, Khaled (2009). *Information Crimes,* Alexandria: University Thought House

- Al-Husseinawi, Ali (2009). *Computer and Internet Crimes*, Amman: Dar Al-Yazouri Scientific for Publishing and Distribution.

- Al-Hajjar Helmy, and Al-Hajjar Rani, 201). *Methodology in resolving conflicts and developing legal studies*, 1st edition, Al-Halabi human rights publications, Beirut, Lebanon

- Al-Janabihi, Mamdouh, (2006). *Internet and computer crimes and means of combating them*. Alexandria: University Thought House.

- Al-Fadil, Muhammad (1962). *Crimes against persons*, second edition, published by Damascus University.

- My void, rich (2015). *Electronic crime, a comparative study* of the publications of the Algerian House: Algeria

- Tawba Abdul Hakim (2009). Information Technology Crimes, 1st Edition, Amman, Dar Al-Mustaqbal for Publishing and Distribution

- Obaid, Emad (2018). *Special Penal Code* Part 2, Syrian Virtual University Publications, Syria

- Al-Sarraj, Abboud (2018). *General Penal Code* Part 1, Publications of the Syrian Virtual University, Syria

- -Nassar, Ghada (2017a). *Terrorism and electronic crime*, Cairo: Al-Araby for Publishing and Distribution.

- **Research :**

- Asmahan, Ben Malak (2019). Characteristics of information crime and the reasons for its commission, *Al-Biban Journal for Legal and Political Studies, Issue 4, pp. 102-124*

- The circumcised, Obaid Saleh (2015). UAE legislator's policy to combat cybercrime. Conditional Thought *Journal, MG. 24, p. 4, pp. 21-52.*

- Al-Ghafri, Hussein, (2007). A study of international efforts in confronting cybercrime,

from *Al-Minshawi Publications for Studies and Research*.

- Al Safar Advocates and Legal Consultants (2022). Combating Cybercrime, an article published *on https://ae.linkedin.com*
- Samira, Maashi (2018). Information Crime "An Analytical Study of the Concept of Information Crime", *Dar Al-Fikr Magazine, Issue 17, pp. 398-417*
- Omar, Ben Yassin (2019). Legal treatment of cybercrime in Algerian and comparative legislation (Moroccan and Emirati legislation as a model), *Journal of Legal and Political Sciences, Volume 10, Issue 3, pp. 710-227.*
- Alkoum, Walid (2000). The concept and phenomenon of information crime, a research submitted to the Law, *Computer and Internet Conference - UAE University*
- Arabs, Younes (2002). Computer and Internet crimes, a working paper presented to the Arab Security *Conference, organized by the Arab Center for Criminal Studies and Research*
- Fatih Raad & Awwad Yasser (2017). Evidence of electronic crime with scientific evidence, *Tikrit University Journal of Law, Issue 3, Part 2*
- *Palestinian Institute for Political and Economic Studies* (2012). A critical study of the legal framework for cybercrime in the Palestinian territories.
- Mohamed Abdel Rahim (2015). A study of cybercrime in Gulf society and how to confront it, retrieved from *http://dr-ama.com/wp-content/uploads/2019/1*

**theses:**

- Al-Ajmi , Dughmush (2014). Practical and legal problems of cybercrime, a comparative study, master's thesis, from the *Middle East University publications.*
- Al-Batati Muhammad (2002). Interest Protected by Criminalization, Ph.D. thesis, *College of Law, University of Mosul*
- Abu Jamea, Osama (2016). Adapting the Criminal Incident in the Palestinian Penal Law, "An Analytical Study", Master Thesis, from the publications of the Faculty of Law, *Al-Azhar University, Gaza, Palestine*
- Saleh bin Mansour, and Anissa Kush (2015). Criminal Behavior of the Cybercriminal, Master Thesis, *Abdelrahman Mirah University, Algeria*.