المواجهة الإدارية والقضائية للجريمة الواقعة على النظام المعلوماتي

رؤية مستقبلية على ضوء القانون اليمني النافذ والمقارن

عبد العالم حسين الفقيه
كلية الشريعة والقانون – جامعة البيضاء
قسم الشريعة والقانون -جامعة السعيدة
abdulalemfk@gmail.com

الملخص

هدفت هذه الدراسة إلى بيان مفهوم الجريمة المعلوماتية وأركانها وخصائصها. والكشف عن أنواع الجريمة الواقعة على النظام المعلوماتي، والتعرف على المواجهة الإدارية والقضائية الحالية للجريمة المعلوماتية في الجمهورية اليمنية. وكذلك محاولة إيجاد رؤية مستقبلية لمواجهة الجريمة الواقعة على النظام المعلوماتي في الجمهورية اليمنية. وفيما يتعلقُ بمنهجِ الدراسةِ، ولتحقيق أهداف الدراسة فقد استخدم الباحث المنهجَ الوصفي التحليلي والمقارن كونهما من المناهج التي تتناسب مع دراستنا الحالية. **وتوصلت الدراسة إلى أهم النتائج التي نورد أبرزها على النحو الآتي**: كشفت الدراسة عن خلو القانون الجنائي اليمني الموضوعي والإجرائي من ذكر أي أحكام خاصة بمواجهة الجريمة الواقعة على النظام المعلوماتي. وعدم وجود تشريع جنائي خاص يواجه الجريمة الواقعة على النظام المعلوماتي. بينت الدراسة عن وجود عدد من مشاريع لقوانين خاصة بمكافحة جرائم تقنية المعلومات لسنة 2018 وسنة 2020م ولم تصدر بعد. كما توصلت الدراسة إلى رؤية حديثة للمواجهة الإدارية والقانونية لتلك الجريمة.

الكلمات المفتاحية: الجريمة المعلوماتية، الجريمة الواقعة على النظام المعلوماتي، المواجهة الإدارية والقضائية.

Administrative and Judicial Confrontation of Crimes Against the Information System "A Future Perspective in Light of the Current and Comparative Yemeni Law"

Abdel Alem Hussein Al-Faqih
Faculty of Sharia and Law - Albaydha University
Department of Sharia and Law - Al-Saeeda University
abdulalemfk@gmail.com

Abstract

This study aims to clarify the concept of information crime, its pillars, and characteristics. It seeks to uncover the types of crimes against the information system, to understand the current administrative and judicial confrontation of information crimes in the Republic of Yemen, and to try to establish a future vision for confronting crimes against the information system in the Republic of Yemen. Concerning the study methodology, to achieve the study's objectives, the researcher used the descriptive, analytical, and comparative method as they are suitable for our current study.

The study concluded the following key results:

- The study revealed the absence of any special provisions in the substantive and procedural Yemeni criminal law regarding confronting crimes against the information system, and the lack of specific criminal legislation addressing crimes against the information system.

- The study indicated the existence of several draft laws for combating information technology crimes from 2018 and 2020, which have not yet been issued.

- The study also presented a modern vision for the administrative and legal confrontation of these crimes.

***Keywords**: Information crime, crimes against the information system, administrative and judicial confrontation.*

مقدمة

تتزايد الجريمة المعلوماتية في اليمن، ولا سيما تلك الواقعة على النظام المعلوماتي نتيجة التطور في شبكة المعلومات العالمية الانترنت، تلك التي تتطور تطبيقاتها وبرامجها باستمرار وبوتيرة عالية، ومع تطور تلك التطبيقات والبرامج تتطور معها بلاشك الجريمة، وهذا يستدعي قيام الدول بتحديث الوسائل القانونية الحديثة لمواجهة تلك الجرائم من الناحية الإدارية من خلال إيجاد وسائل الحماية اللازمة لمواجهة تلك الجرائم إداريًا، بالإضافة إلى تعزيز الوسائل القضائية من أجل كشف تلك الجرائم وإثباتها وتعزيز وسائل التحقيق الجنائي والمحاكمة، وذلك للحد من تلك الجرائم التي تأثر على المجتمع.

وتأسيساً على ما سبق، سنتناول دراسة هذا الموضوع الموسوم بـ " **المواجهة الإدارية والقضائية للجريمة الواقعة على النظام المعلوماتي " وفق رؤية مستقبلية على ضوء القانون اليمني النافذ والمقارن**، ومن هذا المنطلق سنبين فيه مشكلة البحث وأهميته وأهدافه، وكذلك خطة البحث على النحو التالي:

أولاً: أهمية البحث:

تكمُن أهمية البحث في كونه يتناول دراسة موضوع مهم وشائع في المجتمع خاصة بعد انتشار الجرائم المعلوماتية تلك التي تستهدف النظام المعلوماتي للدولة أو للأفراد، ومنهم رجال الأعمال التي تتعرض أنظمتهم لتلك الجرائم، وتعرضهم لمحاولة الابتزاز من قبل الجناة في تلك الجرائم، بالإضافة إلى تعرض شرائح المجتمع المختلفة لتلك الجرائم الخطيرة، ومؤدى ذلك يتعين علينا أن نبحث في تلك الجريمة ومحاولة الوصول إلى معالجات مستقبلية، في ضوء غياب نص تشريعي صريح يعاقب عليها.

ثانياً: مشكلة البحث:

تكمن مشكلة البحث في أن الجرائم المعلوماتية التي تقع على الأنظمة الإلكترونية تعد من الجرائم المستحدثة التي شاعت بعد التطور الكبير الذي حصل في تكنولوجيا المعلومات والتقنية الحديثة، وتتطور بسرعة فائقة في ظل غياب التشريعات اليمنية الكافية التي تحد من تلك الجرائم، وتعمل على تنظيم إجراءات جمع الاستدلالات والتحقيقات فيها، علاوة على صعوبة إثبات هذه الجريمة باعتبارها من الجرائم الجديدة نتيجة الخلو التشريعي والقصور الإداري والقضائي في مواجهة تلك الجريمة، كما أن للجرائم المعلوماتية آثار خطيرة على المجتمع، وتؤثر بشكل كبير في أغلب مناحي الحياة ومنها الاقتصادية والأمنية والاجتماعية وغيرها، ولذلك تتلخص المشكلة في الرد على التساؤل الرئيس الآتي:

ماهي المواجهة الإدارية والقضائية للجريمة الواقعة على النظام المعلوماتي وفق رؤية مستقبلية؟

ثالثاً: تساؤلات البحث:

يتفرع عن السؤال الرئيس للمشكلة الأسئلة الفرعية الآتية:

1- ماهي الجريمة المعلوماتية وخصائصها؟
2- ماهي أنواع الجريمة الواقعة على النظام المعلوماتي؟
3- ماهي المواجهة الإدارية الحالية للجريمة المعلوماتية في الجمهورية اليمنية؟
4- ماهي المواجهة القضائية الحالية للجريمة المعلوماتية في الجمهورية اليمنية؟
5- ماهي الرؤية المستقبلية لمواجهة الجريمة الواقعة على النظام المعلوماتي في الجمهورية اليمنية؟

رابعاً: أهداف البحث:

نهدف من خلال البحث إلى الآتي:

1. بيان مفهوم الجريمة المعلوماتية وخصائصها.
2. التعرف على الجريمة الواقعة على النظام المعلوماتي وأنواعها.
3. مدى كفاية المواجهة الإدارية في الجمهورية اليمنية.
4. الكشف عن وسائل المواجهة القضائية للجريمة المعلوماتية في الجمهورية اليمنية.
5. مدى كفاية التشريعات اليمنية لمواجهة تلك الجريمة.
6. الوصول إلى رؤية قانونية وإدارية وقضائية مستقبلية قادرة على مواجهة تلك الجريمة.

خامساً: أسباب اختيار الموضوع:

1. وجود قصور تشريعي لدى القانون اليمني في تجريم الجرائم الواقعة على النظام المعلوماتي في ظل خلو القانون الجنائي عن تشريع قانوني خاص بمكافحة الجرائم المعلوماتية والتقنية.
2. وجود قصور معرفي لدى المجتمع في كيفية التعامل مع تلك الجرائم.
3. قلة الخبرات التقنية في حماية الأنظمة المعلوماتية.
4. قلة الخبرات الضبطية القادرة على كشف تلك الجرائم وإثباتها والتحقيق فيها لدى أجهزة إنفاذ القانون في اليمن.

سادساً: منهجية البحث:

المنهج الوصفي التحليلي:

من خلال الاطلاع على النصوص القانونية اليمنية النافذة التي تواجهه الجريمة المعلوماتية، مع محاولة الشرح والإيضاح والتحليل ونقد تلك النصوص إذا استدعى الأمر ذلك، من أجل الوصول إلى تشريعات ووسائل كافية للمواجهة المستقبلية.

المنهج المقارن:

من خلال مقارنة الأحكام القانونية المتعلقة بالجريمة المعلوماتية وفقاً لما جاء بالقانون اليمني النافذ ومقارنتها بأهم ما جاء في بعض القوانين العربية ومحاولة استخلاص النتائج العلمية والعملية المناسبة للتطبيق في اليمن.

سابعاً: صعوبة البحث:

تكمن صعوبة البحث في الآتي:

1. خلو التشريع الجنائي من وجود قانون خاص لمكافحة الجرائم المعلوماتية.
2. تدني مستوى التعاون مع الباحثين على مستوى القطاع الحكومي والخاص.
3. قلة الأحكام القضائية اليمنية في الجرائم المعلوماتية.

ثامناً: تقسم خطة البحث:

نتناول هذا الموضوع في أربعة مباحث يسبقها مقدمة وتلحقها خاتمة تتضمن أهم النتائج والتوصيات.

المبحث الأول: مفهوم الجريمة المعلوماتية الواقعة على النظام المعلوماتي.

المبحث الثاني: المواجهة الإدارية للجريمة المعلوماتية الواقعة على النظام المعلوماتي.

المبحث الثالث: المواجهة القضائية للجريمة المعلوماتية الواقعة على النظام المعلوماتي.

المبحث الرابع: الرؤية المقترحة لمواجهة الجريمة المعلوماتية الواقعة على النظام المعلوماتي

المبحث الأول: مفهوم الجريمة المعلوماتية الواقعة على النظام المعلوماتي

تمهيد وتقسيم:

سنتناول مفهوم الجريمة المعلوماتية وخصائصها، ثم نستعرض مدلول وطبيعة الجريمة الواقعة على النظام المعلوماتي، ونبين أنواعها، وذلك في المطلبين الآتيين.

المطلب الأول: تعريف الجريمة المعلوماتية وخصائصها

1. الجريمة المعلوماتية:

تعد من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية نتيجة التطور المسارع الذي ارتبط بتقنية المعلومات، فقد اصطلح على تسميتها بداية " بأساة استخدام الكمبيوتر"، ثم "احتيال الكمبيوتر"، فالجريمة المعلوماتية، وبعدها جرائم الإنترنت، والجرائم الإلكترونية وغيرها **(الزعبي، 2002، ص46)**. هذا وقد تعددت تعاريف الجريمة الإلكترونية وتباينت فيما بينها ضيقًا واتساعًا، ولعل سبب ذلك هو اختلاف التكييف القانوني للجريمة أو الإشكاليات التي قد ظهرت في تكييفها والمحاولات التي بذلت في تعريفها؛ مما أدى إلى انقسام الفقهاء إلى اتجاهين في بيانها: فالاتجاه الأول اتجاه ضيق في تعريف الجريمة الإلكترونية، والاتجاه الثاني الموسع في تعريفها، وظهر اتجاه ثالث حاول الجمع بين الاتجاهين، وهذا ما سنوضحه في الآتي:

أ. الاتجاه المضيق: يرى هذا الاتجاه، إلى عدم ضرورة التفرقة بين الجرائم التي ترتبط بالحاسب الآلي وتلك التي لا ترتبط به، فالحاسب الآلي ما هو إلا وسيلة لارتكاب الجريمة المعاقب عليها، ووفقاً لهذا فالجريمة عندهم:" هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تلك التي يتم تحويلها عن طريقه" **(رستم، 2019، ص 78)** وقد ورد تعريفها أيضاً حسب هذا الرأي بأنها:" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسوب الآلي بقدر كبير لازماً لارتكاب الجريمة" **(قوره، 2004، ص 21)**

وحسب ما سبق نجد أن هذا الاتجاه يستند إلى معيار شخصي، حيث يتوجب من خلال هذا الاتجاه أن يكون الفاعل مُلماً بتقنية المعلومات واستخدام الحاسب الآلي، أي يتوجب توافر المعرفة بتقنية الحاسوب والمعلومات.

ب. الاتجاه الموسع: على عكس الاتجاه السابق يذهب فريق آخر من الفقهاء إلى توسيع مفهوم الجريمة المعلوماتية، ويرى هذا الاتجاه ضرورة التدخل التشريعي لمواجهة هذه الجرائم نظراً لما تتميز به عن غيرها من الجرائم، فوسعت مفهومها لتشمل الاعتداءات المادية على جهاز الحاسوب ذاته أو المعدات المتعلقة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وتحويل الحسابات المالية بطرق إلكترونية، وأيضاً السرقات المادية للجهاز أو أي مكون من مكوناته، فعرفت الجريمة الإلكترونية بأنها:" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها سواءً استخدم الحاسب لتسهيل الجريمة أو وقعت الجريمة على الحاسب ذاته أو أياً من مكوناته" **(أحمد، 1997، ص14)**. وعُرفت أيضاً بأنها:" كل فعل أو امتناع عن فعل عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات ويهدف إلى الاعتداء على الأموال المادية والمعنوية" **(الشوا، 1994، ص 7)**.

ج. الاتجاه الثالث: عرف الجريمة الإلكترونية أو المعلوماتية على أنها:" أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تمثل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية" **(مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين،2000: 78)**. وكذلك عُرفت:" بأنها سلوك غير مشروع يرتبط بأساة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة" **(حجازي، 2007، ص386)**. وتعرف قانونيًا بأنها: "المخالفات التي ترتكب ضد الأفراد أو المجموعات بدافع الجريمة وبقصد إيذاء سمعة الضحية أو أي أذى مادي أو نفسي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات والمعلوماتية"**(العوادي،2016، ص10)**. وجاء تعريفها في مشروع القانون اليمني بلفظ (جرائم تقنية

المعلومات)، بأنها:" كل فعل أو امتناع عن فعل يُرتكب باستخدام أي وسيلة من وسائل تقنية المعلومات، بالمخالفة لأحكام هذا القانون والقوانين النافذة" **(مشروع القانون اليمني الخاص بجرائم تقنية المعلومات، 2020)**

ومن كل ما سبق بيانه، لم نجد تعريف مانع جامع للجريمة المعلوماتية يبين ماهيتها ويوضح خصائصها، وأي من التعريفات السابقة لم يلق نجاح حتى الآن، فبعضهم من عول على فاعل الجريمة ووجوب معرفته بتقنية المعلومات والحاسوب، والبعض استند إلى الوسيلة التي تُرتكب بها الجريمة، ومزج البعض بين التعريفات وهو الموفق حسب ما نراه، وبذلك يصح القول: إن تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة يعد من التعاريف الواضحة والدقيقة.

ثانياً: خصائص الجريمة المعلوماتية:

سبق القول إن الجريمة المعلوماتية تتميز بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بالحاسب الآلي، وتعد إفرازاً ونتاجاً طبيعيا لتقنية المعلومات، وقد استدعت السياسة الجنائية الحديثة محاولة حصر خصائص تلك الجريمة والتي تتسم بلوناً وطابعاً قانونياً خاصاً يميزها عن غيرها من الجرائم، ولعل أبرز خصائص الجرائم المعلوماتية ما يلي:

1. **خطورة الجريمة:** وتتحقق الخطورة من خلال مساسها بالإنسان في فكره وحياته الخاصة، وتمس المؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي، ومن شأن ذلك أن يضفي أبعاداً خطيرة غير مسبوقة على حجم الأضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات، وتُعتبر البنوك الهدف الرئيسي للجيل الجديد من مجرمي تقنية المعلومات، وذلك لاعتمادها كلياً على أنظمة نقل التمويل إلكترونياً **(أبكر، 1420، ص47)**.
2. **جرائم ناعمة وسهلة التنفيذ:** إذا كانت الجريمة بصورتها التقليدية تحتاج في الأغلب إلى مجهود عضلي من الجاني كجرائم القتل أو السرقة أو الاغتصاب مثلاً، فإن الجريمة الإلكترونية على العكس لا تحتاج إلى أدنى مجهود عضلي، بل تعتمد على الدراية الذهنية والتفكير العلمي المدروس القائم على المعرفة بتقنيات الحاسب الآلي، وآلية تشغيله، بالإضافة إلى الإحاطة ببعض البرامج التشغيلية **(أبكر، 1420، ص 48)**. أي أنها سهلة أثناء القيام بارتكابها وتحتاج إلى معرفة وحاسب آلي أو جهاز تلفون ذكي.
3. **جرائم سريعة التنفيذ:** من الإغراءات التي تجذب المجرمين نحو هذه الجرائم أنها جرائم سريعة التنفيذ، إذ غالباً ما يتمثل الركن المادي فيها باستعمال جهاز الحاسب الآلي، مع إمكانية تنفيذ ذلك عن بعد دون اشتراط التواجد على مسرح الجريمة، فضلاً عن ضخامة الفوائد والمكاسب التي يستطيع الجاني تحقيقها في اقل وقت وأقل جهد **(رستم، 1994، ص23)**.
4. **صعوبة اكتشاف الجريمة:** يرجع السبب في صعوبة اكتشاف ارتكاب الجريمة المعلوماتية ذات الطابع التقني إلى أنه من السهل إخفاء معالم تلك الجريمة وصعوبة تتبع مرتكبيها، كما أن هذه الجرائم لا تترك أثراً لها بعد ارتكابها، علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت، فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات، ولذا فإن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابها، كما لا يتم في الغالب الإبلاغ عن تلك الجرائم؛ أما لعدم اكتشاف الضحية لها، وإما خشية المجني عليه من التشهير، وفي الواقع فإن من أهم الأسباب وراء صعوبة اكتشاف هذه الجرائم؛ يرجع إلى أنها لا يشوب ارتكابها أي عمل من أعمال العنف، وإلى الطابع التقني الذي يضفي عليها غالباً الكثير من التعقيد، وخلو تلك الجرائم من مسرح للجريمة فعلي بل افتراضي **(الصغير، 1992، ص17)**.
5. **صعوبة إثبات الجريمة:** يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية وسلطة التحقيق، ويزداد الإثبات صعوبة في الجريمة المعلوماتية، حيث إن اكتشاف تلك الجريمة أمر ليس بالسهل، فالجريمة تتم في بيئة غير تقليدية، حيث تقع خارج إطار الواقع المادي الملموس، مما يجعل الأمور تزداد تعقيداً لدى سلطات أنفاذ القانون، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي، كما إن وسائل المعاينة وطرقها التقليدية لا تفلح غالباً في إثبات هذه الجريمة؛ نظراً لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالأخيرة لها مسرح تجري عليه الأحداث حيث تخلف آثاراً مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الاستدلال والتحقيق الجنائي في الكشف عن الجريمة؛ وذلك عن طريق المعاينة والتحفظ على الآثار المادية التي خلفتها الجريمة، لكن فكرة مسرح الجريمة في الجريمة محل الدراسة يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة وذلك لسببين، الأول: أن الجريمة المعلوماتية لا تختلف آثارها المادية. والثاني: أن العديد من الأشخاص يترددون على مسرح الجريمة الافتراضي خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها أو التحقيق فيها وهي فترة طويلة نسبياً. الأمر الذي يعطي مجالاً للجاني أو للآخرين أن يغيروا أو يتلفوا ويعبثوا بالآثار المادية إن وجدت، مما يؤدي إلى الشك في حقيقة الأدلة المستقاة من المعاينة في تلك الجريمة، بالإضافة إلى نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء في الدول النامية يشكل عائقاً أساسياً أمام إثبات الجريمة المعلوماتية **(حجازي، 2002، ص60)**.

6. خصوصية مجرمي المعلومات: المجرم الذي يقترف الجريمة المعلوماتية والذي يطلق عليه مصطلح المجرم المعلوماتي، يتسم بخصائص معينة تميزه عن المجرم الذي يقترف الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا أثر فيها للمستويين العلمي والمعرفي للمجرم في عملية ارتكابها باعتبارها قاعدة عامة، فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية تقنية في الغالب الأعم، ومن يرتكبها عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو على الأقل شخص لدية حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت **(الموشير، 2009، ص20).**

ومن أهم ما يُميز المجرم المعلوماتي أنه مجرم يتمتع بذكاء حاد، لا نجد هذا الذكاء في المجرمين التقليديين- الذين في الغالب ما يتركوا أثراً ليدل عليهم- بخلاف المجرم الإلكتروني فقد ألم بجميع الجوانب الفنية والتقنية لجريمته، مما يساعده في التخلص من أدلة إدانته في وقت سريع وبأقل جهد **(إبراهيم، 2009، ص134).**

7. جرائم عبر الوطنية (دولية): إن من أهم الخصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها: إن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، فتلك الجرائم لم تعد تقتصر على إقليم معين ولا تتعداه، بل أصبح بالإمكان ارتكاب الجرائم عن طريق الكمبيوتر باختراقه لكمبيوتر آخر في بلد آخر أو إتلاف معطياته، فالتعدي يتم في بلد وأثره يقع في بلد آخر**(محمود، 2001، ص 12).**

وتأسيساً لما سبق، نجد أن تلك الجرائم تتمتع بخصائص تختلف عن الجرائم التقليدية من حيث خطورتها وسرعة تنفيذها وصعوبة اكتشافها وإثباتها، بالإضافة إلى أنها جرائم عابرة للدول وتحدث عبر الشبكة المعلوماتية (الإنترنت).

المطلب الثاني: مدلول الجريمة الواقعة على النظام المعلوماتي وأنواعها

من سوء الطالع أن يتم التعامل مع هذه الجرائم وفقاً للقانون اليمني على أنها من الجرائم التقليدية مع مضي عقدين من الزمن على ظهور تلك الجرائم، وبالتالي يسأل مرتكبها بموجب نصوص قانون الجرائم والعقوبات الذي لم يتطرق إلى تلك الجرائم البته رغم التعديلات المتعاقبة التي جرت على التشريعات اليمنية، وهذه الاعتداءات على المكونات المادية للنظام المعلوماتي لا تشكل أي صعوبة، بينما تتحقق الصعوبة في الجرائم الواقعة على المكونات المنطقية (المعنوية) للنظام المعلوماتي، فتقوم الجريمة المعلوماتية إذا كانت المكونات المنطقية للنظام المعلوماتي متمثلة بالمعلومات بكل صورها، هي محل الاعتداء فقد تتم سرقة هذه المعلومات أو إتلافها أو تزويرها وغيرها من الأفعال غير المشروعة. هذا وقد جاء في قانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية اليمني في مادته الأولى تعريف نظام معالجة المعلومات: (بأنه المنظومة الإلكترونية المستخدمة لإنشاء رسائل البيانات ومعالجتها وتجهيزها وتخزينها وإرسالها واستقبالها) كما عُرف تبادل البيانات الإلكترونيات بأنها: "نقل البيانات إلكترونياً من شخص إلى آخر باستخدام نظام معالجة المعلومات". غير أن ما يلاحظ على ذلك القانون أنه لم يتناول الجريمة الواقعة على النظام المعلوماتي بشكل صريح.

ونظراً لعدم وجود تعريف للجريمة الواقعة على النظام المعلوماتي فسنعرفها إجرائياً على أنها" تلك الجرائم الواقعة على الحاسب الإلي من خلال شبكة الأنترنت وتستهدف الدخول غير المشروع لأي نظام معلوماتي يجب ألا يطلع عليه غير المختص، بهدف الحصول على تلك المعلومات أو أتلافها والعبث بمحتواها وحرمان من يملكها من استخدامها والانتفاع بها". وبناء على ما سبق فسنكتفي في هذا المطلب بتناول أنواع الجرائم الواقعة على المكونات (المعنوية) للنظام المعلوماتي، بحسب بيانها وفقاً للقواعد العامة في التشريع اليمني ومشروع قانون مكافحة الجرائم المعلوماتية لسنة 2018م والمعدل في 2020، وذلك على النحو الآتي:

أولاً: الدخول والبقاء غير المشروع:

يتعرض النظام المعلوماتي إلى الاختراق من قبل أفراد غير مصرح لهم بالدخول إليه أو البقاء فيه، وقد ساهم في انتشار هذه الظاهرة تطور الاتصالات وتنامي الشبكات المعلوماتية، بحيث يعد هذا الفعل مرحلة سابقة وضرورية لارتكاب الجرائم المعلوماتية الأخرى، مثل سرقة المعلومات وتزويرها، أو التجسس المعلوماتي أو الاحتيال المعلوماتي، وقد اثارت هذه الحالة خلافاً في الفقه حول مدى انطباق وصف الجريمة المعلوماتية عليها وبالتالي إذا كانت تستوجب الحماية الجنائية أو لا؟ **(المومني، 2010، ص156).**

ويقصد بالدخول غير المصرح به:" فعل الولوج والتواجد بالنظام بهدف الاطلاع على المعلومات المخزنة به واستغلالها أو التواصل معها بأي وجه دون المساس المادي بحق ملكية الغير" **(عبد الحكيم، 2015، ص215).** أما فعل البقاء غير المشروع فيقصد به:" التواجد داخل هذا النظام بالمخالفة لإرادة الشخص أي النظام أو من له السيطرة عليه" **(المومني، ص161).**

وسوف نتناول فعلي الدخول والبقاء غير المصرح به إلى النظام المعلوماتي كلاً على حده، حيث يتفق الفقه على أن الركن المادي يختلف في هذين الفعلين:

1- فعل الدخول غير المصرح به:

الركن المادي: يتمثل بفعل الدخول أو مجرد المحاولة، وفعل الدخول هو سلوك إيجابي، ومحاولة الدخول أيضاً هو سلوك إيجابي مثله مثل فعل الدخول العادي إلا أنه يقتصر على المحاولة دون أن يتمكن الجاني من الدخول الفعلي إلى النظام، ويتخذ فعل الدخول بوصفه جرماً انطلاقاً من كونه قد تم دون وجه حق، لا باعتباره سلوكاً غير مشروع بحد ذاته. ومن هذه الحالات دخول الفاعل دون تصريح من المسؤول عن النظام، وقد يكون مصرح له لكنه يتجاوز التصريح الممنوح له، ويتحقق فعل الدخول إلى النظام سواءً تم بشكل كلي أو جزئي، والحكمة من المساواة بين الولوج الكلي والجزئي وذلك لكبح التدخل المقترن بالغش والتعدي، وتعد جريمة الدخول غير المشروع من الجرائم الشكلية التي لا تتطلب حدوث نتيجة إجرامية معينة، فيكفي فعل الدخول غير المصرح به إلى النظام المعلوماتي ليقوم الركن المادي للجريمة، وبذلك تتساوى مع جرائم الخطر وهي الجرائم التي لا يشترط فيها تحقق النتيجة الإجرامية **(غلاب، 2011، ص186)**.

2- فعل البقاء غير المصرح به:

الركن المادي: في فعل البقاء داخل النظام المعلوماتي له صور متعددة، منها تجاوز الوقت المسموح به للبقاء داخل النظام، أو البقاء بعد وجود الجاني داخل النظام عن طريق الخطأ أو المصادفة، فقد يجد الشخص نفسه داخل نظام الحاسب الآلي غير مرخص له الدخول أو البقاء فيه إلا أنه يستمر في البقاء فيه فيكون بذلك ارتكب جريمة بقاء غير مشروع، وهذا التواجد والبقاء دون إرادة ورغبة صاحبه أو ملكيته، ويتحقق بالدخول غفلة ولو لم يتبعه إتلاف للمعطيات **(غلاب، ص193)**.

وجريمة البقاء غير المشروع من الجرائم الشكلية التي لا تتطلب توافر نتيجة إجرامية معينة، فيكفي توافر فعل البقاء غير المشروع داخل النظام المعلوماتي ليقوم الركن المادي للجريمة.

الركن المعنوي لجريمة الدخول والبقاء غير المشروع: يتحقق من خلال توافر القصد الجنائي العام بعنصريه العلم والإرادة، أي علم الجاني وإدراكه بالدخول غير مشروع واتجاه إرادة إلى ذلك، فإن القصد الجنائي لجريمة الدخول والبقاء ينتفي طبقاً للقواعد العامة ولا يتحقق إذا كان الجاني قد اعتقد خطأ بأنه مازال له الحق في الدخول إلى النظام الآلي، أما في حالة استمراره في البقاء فإن الجريمة تكون عمديه **(حسين، 2017، ص23)**.

- **موقف المشرع اليمني:**

القانون العقابي اليمني لم يتضمن نصوصاً تجرم فعل الدخول غير المشروع إلى النظام المعلوماتي أو البقاء فيه بدون إذن، سواءً ارتكب الفعل بقصد ارتكاب جريمة أو لا، كما أنه لا يوجد نص عقابي في قانون حماية الحقوق الفكرية ينظم هذه الصورة من صور الإجرام، وليس هناك نصوص قانونية تنظم تجريم فعل الدخول والبقاء إلى الانظمة المعالجة الآلية للمعطيات كجريمة مستحدثه. وبالرجوع إلى نصوص قانون العقوبات المتعلقة بانتهاك حرمة الحياة الخاصة نلاحظ فيها:

1. تجريم المشرع الاعتداء على حرمة المسكن بنص المادة (253) عقوبات يمني.
2. الاعتداء على حرمة الخاصة بالأشخاص، أو الالتقاط أو النقل الصور وهذا ما نصت عليه المادة (256) عقوبات يمني.

ومن خلال النصوص السابقة نلاحظ بأنه لا يمكن تطبيقها على جريمة الدخول والبقاء في نظام المعالجة الآلية للمعطيات؛ لكونها لم تتضمن ما يشير من قريب أو من بعيد على تنظيم ذلك النوع من الإجرام ففي حرمة الاعتداء على المسكن يمنع دخولها دون إرادة مالكيها، لأن الدخول في الواقع دخول مادي ملموس، بعكس الدخول والبقاء في نظام الكمبيوتر فهو يمثل دخول معنوي تستخدم فيه تقنية حديثة، ومن نص المادة (256) عقوبات يمني، يبدو بأنها لا تسري على المحادثات المكتوبة بين جهازين من أجهزة الكمبيوتر، إضافة إلى أن فعلي النقل أو الالتقاط في النص قد اقتصر على الصورة وليس البيانات.

بينما مشروع القانون الخاص بمكافحة جرائم تقنية المعلومات اليمني لسنة 2018م، تناول هذه الجريمة في المادة (12) منه، والتي نصت على:"

أ- يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر أو بغرامة لا تقل عن عشرة ألف ريال ولا تزيد على مائة ألف ريال كل من تعمد الدخول أو البقاء بأي وسيلة تقنية المعلومات بدون وجه حق إلى كل أو جزء من نظام المعلومات الإلكتروني.

ب- إذا ترتب على الدخول أو البقاء حذف أو نسخ أو تغيير المعلومات المخزنة في نظام المعلومات الإلكتروني تكون العقوبة الحبس مدة لا تزيد على سنة وبغرامة لا تزيد على مائتي ألف ريال.

ج- وإذا ترتب على الدخول أو البقاء تخريب نظام المعلومات الإلكتروني تكون العقوبة الحبس مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليون ريال".

في حين أن مشروع القانون المعدل سنة 2020م، بشأن مكافحة جرائم تقنية المعلومات اليمني، نصت المادة (6) منه، على أنه:" أ- يعاقب بالحبس مدة لا تزيد عن سنة وبغرامة لا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين كل من دخل دون وجه حق أو تجاوز حدود الحق المخول له من حيث

الزمان موقعاً إلكترونياً أو بريداً إلكترونياً أو حساباً خاصاً أو نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات. ب- فإذا ترتب على أي من الأفعال السابقة إلغاء أو حذف أو نسخ أو تغيير أو تعديل أو إتلاف أو محو أو إضافة أو تعطيل أو تخريب أو إعاقة أو توقيف أو نقل أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على ثمانية مليون ريال أو بإحدى هاتين العقوبتين.". وأما موقف القانون المصري بشأن جريمة الدخول غير المشروع، فقد نصت المادة (14) من قانون مكافحة جرائم تقنية المعلومات، والتي نصت على أنه:" يعاقب بالحبس مدة لا تزيد عن سنة وبغرامة لا تقل على خمسين ألف جنية ولا تجاوز مائة ألف جنية أو بإحدى هاتين العقوبتين كل من دخل عمداً أو دخل بخطأ غير عمدي وبقاء بدون وجه حق على موقع أو حساب خاص أو نظام معلوماتي محضور الدخول عليه. فإذا تنج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف جنية أو بإحدى هاتين العقوبتين." **(القانون رقم (175) لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات المصري).**

ونرى أن على المقنن اليمني ضرورة الإسراع بسن مشروع القانون الخاص بمكافحة جرائم تقنية المعلومات لمواجهة خطر هذه الجريمة وأن يقوم بتعديلات على النصوص العقابية، وأن يراعي في ذلك تدارك القصور الحاصلة في التشريعات المقارنة بهذا الخصوص.

ثانياً: الاستعمال غير المصرح به للنظام المعلوماتي

إن الانتشار الواسع للحواسيب والشبكات المعلوماتية التي تربط بينها، والاعتماد الكبير في سبيل إنجاز الأعمال المختلفة في كافة مجالات الحياة، أوجد معه تساؤلاً حول مدى مشروعية الاستعمال غير المصرح به لهذه الأنظمة من قبل بعض الأفراد، والتكييف القانوني لهذا الفعل، وسنتناول هذه الجريمة ببيان مفهوم الاستعمال غير المصرح به ثم أركان الجريمة، ثم نبين موقف المشرع اليمني والمصري على النحو الآتي:

1- مفهوم الاستعمال غير المصرح: ويقصد بالاستعمال:" هو كل استخدام للحاسب الآلي ونظامه للاستفادة من الخدمات التي يقدمها دون أن يكون للشخص الذي قام بالاستخدام الحق في ذلك" **(غلاب، 198).** وأيضاً يمكن تعريف الاستعمال على أنه:" كل استعمال للوظيفة التي يؤديها الحاسوب خلال فترة زمنية دون أن يكون مصرحًا بذلك الفعل" **(المومني، 2010، ص144).**

2- أركان جريمة الاستعمال غير الصرح به: وهذه الجريمة كغيرها من الجرائم المعلوماتية التي تستلزم لقيامها توافر الركن المادي والمعنوي على النحو الآتي **(محمد، 2017، ص20)**:

الركن المادي: يتمثل السلوك الإجرامي الذي يقوم به الركن المادي، هو فعل الاستعمال غير المشروع وغير المصرح به دون وجه حق على الوظيفة أو الخدمة التي ينظمها الحاسب الآلي، وحدوث النتيجة الجريمة الناتجة عن الاستعمال غير المصرح به، ورابطة السببية بين الفعل أي الاستعمال غير المشروع وحدوث الضرر على المجني عليه أي النتيجة.

الركن المعنوي: لا بد لتحقق هذه الجريمة من توافر الركن المعنوي المتمثل في القصد الجنائي العام الذي يتألف بعنصريه العلم والإرادة علم الجاني بأنه سيستعمل أشياء مملوكة للغير دون رضاه ودون وجه حق، وكذلك اتجاه إرادته إلى إتيان الفعل.

- **موقف المشرع اليمني:**

بهذا الخصوص نود الإشارة إلى أن المشرع اليمني لم يتضمن الاستعمال غير المشروع للجهاز أو النظام المعلوماتي أو الشبكة وعدم وجود نصوص خاصة بالجرائم المعلوماتية، وكذلك لم ينظم الاستعمال كسلوك في القواعد التقليدية غير أن القاضي اليمني يطبق على تلك الجرائم النصوص القانونية الواردة تحت فصل جرائم النشر والعلانية الواردة في قانون الجرائم والعقوبات.

بينما تناول مشروع القانون المعد سنة 2018م بشأن مكافحة جرائم تقنية المعلومات اليمني، هذه الجريمة في المادة (16/أ) منه، والتي نصت على أنه:" أ- يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على أربع سنوات وبغرامة لا تقل عن ثلاثمائة ألف ريال ولا تزيد على مليوني ريال كل من دخل عمداً إلى نظام المعلومات الإلكتروني بقصد الحصول على بيانات أو معلومات حكومية سرية بطبيعتها وفقاً للتشريعات النافذة."، وكذلك في المادة (23) منه، والتي نصت على أنه:" ... فإذا تم استعمالها أو نشرها للحصول على أموال الغير أو الاستفادة من الخدمات التي تقدمها بواسطتها أو القيام بتزوير بطاقة الائتمان أو أي من وسائل الدفع الإلكتروني أو استخدامها، فتكون العقوبة الحبس مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات أو بغرامة لا تقل عن مليون ريال ولا تزيد على خمسة ملايين ريال.". كما إن المادة (19/أ) منه، نصت على أنه:" يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد عن خمس سنوات وبغرامة لا تقل عن خمسمائة ألف ريال ولا تزيد عن مليوني ريال كل من ارتكب عمداً وبدون وجه حق أي من الأفعال التالية: أ- نشر أو حاز أو أفشى أو استعمل البيانات أو المعلومات التي تم الحصول عليها نتيجة ارتكاب إحدى الجرائم المنصوص عليها في هذا القانون.".

بخلاف نظيره المصري الذي تضمن ذلك في المادة (15) من قانون مكافحة جرائم تقنية المعلومات، تحت مسمى جريمة تجاوز حدود الحق في الدخول انه:" يعاقب بالحبس مدة لا تقل عن ستة أشهر أو بغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل موقع أو حساب خاص أو نظام معلوماتي مستخدما حقا مخولا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول".

ونرى أنه لا بد للمقنن اليمني أن يحذو حذو غيره من التشريعات المقارنة بأن يعالج هذه المشكلات والجرائم بوضع نصوص خاصة لخطورة هذه الجرائم، أو الإسراع في إقرار مشروع القانون الخاص بمكافحة الجرائم المعلوماتية لسنة 2018م، والمعدل في لسنة 2021م.

ثالثاً: سرقة المعلومات:

أصبحت المعلومة مصدر قوة ومصدر سلطة حتى قيل إن المعرفة هي سلطة وأن الحصول على المعرفة وضمان استخدامها عاملان أساسيان من عوامل التقدم، ولذلك فإن التكنولوجية الحديثة تتعلق بالمعرفة تعد سلطة **(المؤمني، ص99)**. ولذلك سنعمل على دراسة هذه الجريمة ببيان مفهوم السرقة كجريمة تقليديه ومفهوم السرقة المعلوماتية ثم نتناول الأركان العامة لجريمة السرقة المعلوماتية، وذلك على النحو الآتي:

أولاً: تعريف جريمة السرقة المعلوماتية:

تُعرف السرقة بأنها:" اختلاس مال منقول مملوك للغير بنيه التملك". وقد عرفها القانون اليمني في المادة (294) عقوبات يمني، بأنها:" أخذ نصاب من مال منقول مملوك للغير خفية من حرز مثله بقصد تملكه..."**(قانون الجرائم والعقوبات اليمني لسنة 1994)**.

وجريمة سرقة المعلومات تسمى "جريمة القرصنة المعلوماتية" ويقصد بها:" الاستخدام أو النسخ غير المشروع لنظم التسجيل أو البرامج الحاسب الآلي المختلفة، أي ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونياً" **(المومني، ص 42)**.

ثانياً: الأركان العامة لجريمة السرقة المعلوماتية:

جريمة السرقة التقليدية تقوم على محل يتمثل بأخذ مال منقول مملوك للغير، وركن مادي يتمثل في فعل الاختلاس لنقل ذلك المال إلى حيازة الجاني بدون رضاء حاجبه، وركن معنوي يتمثل في نية تملك المال المختلس، وذلك ما سيتم التطرق إليه لإيضاح مدى تحقق تلك الأركان في جريمة السرقة المنصبة على المعلومات.

موضوع الجريمة (الزنداني، 2019، ص147):

يشترط لتحقق جريمة السرقة أن يكون محلها مالاً، ويشترط في ذلك المال أن يكون منقولاً، وله قيمة، وأن يكون مملوكاً الغير، وبالتالي فلا تقع الجريمة إذا تخلف شرط من الشروط المذكورة وفقاً للقواعد العامة، وهنا نتساءل هل تعد الأشياء المعلوماتية أموال؟ وما طبيعة ذلك المال؟ وهل تعدّ في عداد المنقولات وقابلة للتملك، مثلها مثل الأموال المادية؟

وللإجابة عن تلك التساؤلات يتحتم علينا بيان معنى المال المعلوماتي، إذ يقصد بالمال المعلوماتي المعنوي:" مكونات العناصر المنطقية للنظام المعلوماتي من برامج وبيانات صالحة للاستخدام أي المعالجة الآلية" **(غلاب، ص 88)**.

ونتيجة الخلاف الفقهي بما يعد محل لجريمة السرقة فقد رأى البعض بأن الأشياء المعلوماتية من بيانات ومعلومات وبرامج لا تعد أموال ولا تقوم بالمال ومرد رأيهم إلى طبيعة تلك الأشياء كونها معنوية وليست مادية تخضع للاستغلال والتصرف، وظهر رأي غالب بأن تلك المعلومات هي ذات طبيعة مالية منقولة مملوكة للغير والواقع يشهد بأهميتها في كافة شؤون الحياة الاجتماعية والعسكرية والصناعية والاقتصادية. وبذلك فأننا نؤيد أصحاب الاتجاه الذي يرى أن الأنظمة المعلوماتية مال منقول مملوك للغير، وأن كان ذلك المال له طبيعة معنوية وليست مادية، ومع ذلك فإن خضوع السرقة المعلوماتية للقواعد العامة لجريمة السرقة رهين بتحقق باقي أركان الجريمة، وملائمتها على سرقة المعلومات.

الركن المادي لجريمة السرقة المعلوماتية:

يقوم هذا السلوك أما عن طريق قيام الجاني باختراق الأنظمة المعلوماتية، أو الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية، ونسخ البرامج أو طباعة المعلومات ليضمن عنه صورة للأصل وهو يؤدي عملاً إلا أن فعل الاختلاس إنما يقع على الأصل نفسه وأن يؤدي ذلك الفعل من حرمان صاحبه من المنفعة منه **(الجنيد، 2021، ص265)**.

وهنا نود القول إن السرقة المعلوماتية تتمثل في نشاط الجاني أي المجرم المعلوماتي في الحصول غير المشروع على ملك الغير وذلك المال وأن كان مال معنوي إلا أنه يقوم بمال لا يختلف عن المال التقليدي، وتتحقق النتيجة في أخذ ذلك المال مع توافر علاقة السببية بين فعل الجاني والنتيجة الإجرامية الافتراضية.

الركن المعنوي لجريمة السرقة المعلوماتية:

يتمثل القصد الجنائي بعلم الجاني بالعناصر المكونة للجريمة، فيجب أن يعلم الجاني بأنه يقدم على فعل يجرمه القانون، ومن شأنه الاعتداء على المال المعلوماتي، سواءً تمثل بفعل الدخول إلى النظام أو البقاء فيه أو أي فعل آخر يتوصل به الجاني إلى سرقة المعلومات كفعل الالتقاط الذهني أو الاعتراض للمعلومات أثناء تبادلها وانتقالها من نظام إلى آخر شريطة أن ينص القانون على تجريم تلك الأفعال، وأن يعلم الجاني بأنه

يقوم باختلاس معلومات مملوكة للغير وبدون رضاء صاحبها، وبالتالي فإن القصد ينتفي في حالة إذا كانت المعلومات متاحة للكافة، وتوافر الإرادة باقتراف تلك الأفعال وأن تتجه إرادة الجاني إلى تحقيق النتيجة الإجرامية، وبالعلم والإرادة يتحقق القصد الجنائي العام، ويتوفر القصد الجنائي الخاص في جريمة سرقة المعلومات قرينة التملك للشيء محل الاعتداء وتبديل حيازتها وممارسة سلطات المالك عليها **(غلاب، ص109).**

- **موقف المشرع اليمني:**

سبق القول إنه لا توجد نصوص خاصة تنظم الجرائم المعلوماتية في اليمن بما فيها جريمة السرقة المعلوماتية، إلا أن القواعد القانونية العامة تتضمن السرقة التقليدية ولبحث مدى انطباق النصوص التقليدية على السرقة المعلوماتية وفي ضوء الخلاف الفقهي القائم بهذا الخصوص، لا بد من التفرقة بين الأموال المعلوماتية المادية والأموال المعلوماتية المعنوية.

1. الأموال المعلوماتية المادية:

الأموال المعلوماتية المادية مثل جهاز الحاسوب وتوابعه من الأجهزة والبرامج وغيرها من المكونات المادية، فلا خلاف حول خضوعها لنص المادة (294) عقوبات يمني، وهذا ما أشرنا إليه في بداية المطلب.

2. الأموال المعلوماتية المعنوية:

من خلال المقارنة يمكن التوصل إلى نتيجة، تتمثل في عدم إمكان تطبيق نصوص قانون الجرائم والعقوبات اليمني وفقاً للرأي القائل بعدم تحقق سرقة المعلومات إلا إذا اقترنت بالوعاء الذي يحتويها **(غلاب، ص114).**

وقد تناول مشروع قانون مكافحة جرائم تقنية المعلومات اليمني لسنة 2018م، في المادة (20) منه، والتي نصت على أنه:" يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على سبع سنوات وبغرامة لا تقل عن مليون ريال ولا تزيد على أربعة ملايين ريال كل من استولى أو تحصل لنفسه أو لغيره على مال منقول أو منفعة أو على سند أو توقيع هذا السند عبر الشبكة المعلوماتية أو بأي وسيلة من وسائل تقنية المعلومات بطرق احتيالية أو باتخاذ اسم كاذب أو انتحال صفة.".

في حين أن مشروع القانون سنة 2020م بشأن مكافحة جرائم تقنية المعلومات اليمني، فقد نصت في المادة (12/ج) منه، على أنه:" ج- فإذا توصل من ذلك إلى استيلاء لنفسه أو لغيره على تلك الخدمات أو أموال الغير فتكون العقوبة الحبس الذي لا يزيد مدته على سبع سنوات وبغرامة لا تزيد على عشرة ملايين ريال، أو بإحدى هاتين العقوبتين.". ومما يصح القول إن المشروع اليمني كان أكثر وضوحا في تحديد محل الجريمة والعقوبة.

أما بالنسبة للتشريع المصري فقد أورد جريمة السرقة الإلكترونية في قانون مكافحة جرائم تقنية المعلومات لسنة 2018، في المادة (23) والتي نصت على أنه:" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر أو بغرامة لا تقل عن ثلاثين ألف جنية ولا تجاوز خمسين ألف جنية أو بإحدى هاتين العقوبتين كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية. فإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر بغرامة لا تقل عن خمسين ألف جنية ولا تجاوز مائتي ألف جنية أو إحدى هاتين العقوبتين. وتكون العقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن مائة ألف جنية ولا تجاوز مائتي ألف جنية أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير." **(مكافحة جرائم تقنية المعلومات المصري، 2018).**

وعلى العكس من ذلك جاء القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية اليمني خالية نصوصه من تجريم الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الإلكترونية كما فعل المقنن المصري، بل لم يشير إلى جريمة سرقة المعلومات ولم يضع لها أي عقاب وكان الأولى به أن يتناولها في نصوصه نظرا لزيادة مثل تلك الجرائم من حيث الواقع.

ونحن نرى إمكانية تطبيق النصوص التقليدية الخاصة بالسرقة على السرقة المعلوماتية وذلك للخلاف القائم بخصوص ذلك في الفقه القانوني، ومع ذلك نقترح تعديل نصوص القانون رقم 40 لسنة 2006 وإجراء التعديلات اللازمة أسوة بتشريعات الدول العربية ولاسيما التشريعات المصرية.

رابعاً: جريمة إتلاف المعلومات:

الإتلاف هو:" تخريب الشي موضوع الجريمة، وذلك بجعله غير صالح للاستعمال أو الانتفاع به أو التقليل من منفعته" **(الغزواني، د. ن، ص57).** أما فعل الإتلاف في مجال المعلوماتية فقد تقع على المكونات المادية للنظام المعلوماتي، وقد تقع على المكونات المنطقية المعنوية لهذا النظام المتمثلة في المعلومات دون أن يؤدي ذلك إلى إتلاف أي عنصر مادي.

أولاً: التمييز بين إتلاف المكونات المادية والمعنوية للنظام المعلوماتي:

1. إتلاف المكونات المادية:

إتلاف النظام المعلوماتي بمكوناته المادية، مثل أجهزة الحاسب وشاشات العرض، والكابلات ولوحة المفاتيح والأقراص الممغنطة، وغير ذلك من المكونات ذات الطبيعة المادية، سواءً كانت تحوي برامج أو كانت خالية من البرامج فإن مثل هذه المسالة لا تثير أية مشكلة، في إمكانية تطبيق النصوص

التقليدية عليها لكونها تدخل ضمن الأموال، ولا خلاف في هذه المسالة.

2. إتلاف المكونات المعنوية:

يثور الخلاف حول مدى انطباق النصوص التقليدية على المكونات المنطقية المعنوية للنظام المعلوماتي؟ وبهذا الخصوص فقد وجد خلاف بين مؤيد ومعارض ولكلاً منهم المبررات والأسباب التي يحتج بها، فالمؤيد يرى أنه لا يوجد ما يحول دون وقوع جريمة الإتلاف على برامج وبيانات النظم المعلوماتية، وبالتالي انطباق النصوص التقليدية عليها مبرراً ذلك في وصف المال بأنه مادي، وأن المعلومات أياً كانت صورتها فإن الطبيعة المالية لها تمثل الجانب الأكبر، وأن نصوص التقليدية وردت عامة لا تفرق بين الأموال المادية، والأموال المعنوية، وغيرها، أما الاتجاه المعارض فيرى عدم وقوع جريمة الإتلاف على المكونات المنطقية المعنوية للنظام المعلوماتي، وبالتالي عدم إمكانية تطبيق النصوص التقليدية عليها لعدة مبررات تعكس ما برر به أصحاب الاتجاه المؤيد، والنتيجة فتظهر عدم انطباق النصوص التقليدية على إتلاف البيانات والبرامج المعلوماتية، باعتبار تلك النصوص تضمنه على الأشياء ذات الطبيعة المادية **(غلاب، ص149).**

ثانياً: أركان جريمة الإتلاف المعلوماتي:

محل الجريمة: تقع على المكونات المنطقية المعنوية للنظام المعلوماتي، وهي بهذا المحل تكون أدق من جريمة السرقة التقليدية وأعمالها بهذه الصورة هو الأصح.

الركن المادي: يتمثل بالنشاط الإجرامي ولهذا النشاط عدة صور منها الإدخال غير المشروع للمعلومات أي إدخال معطيات موجودة مسبقاً بقصد التشويش على صلة المعلومات والبيانات وهي أفعال المحو إزالة جزء من المعطيات المسجلة على دعامه الموجودة داخل النظام أو تحطيم تلك الدعامة، والتعطيل توقف الشيء عن القيام بوظيفته فترة مؤقتة، والتخريب توقف الشيء تماماً عن القيام بمنفعته كلياً أو جزئياً، والتعديل إجراء نوع من التغيير غير المشروع للمعلومات والبيانات المحفوظة داخل النظام واستبدالها بمعطيات ومعلومات جديدة **(محمد، ص17).**

الركن المعنوي: يلزم لقيام الجريمة توافر القصد الجنائي العام بعنصريه العلم والإرادة، أي يجب أن يعلم الجاني بأنه يتلف برامج حاسب آلي خاصة لشخص آخر وذلك بإفسادها أو تخريبها أو تعطيلها، وفي نفس الوقت تتجه إرادته لارتكاب هذا الفعل، أما إذا كان الإتلاف غير مقصود فيما لو حدث أمر عارض أدى إلى افساد برامج الحاسب الآلي، فإن الفاعل يسأل عن خطئه أو إهماله أو تقصيره فقط **(الغزواني، ص91).**

- **موقف المشرع اليمني:**

نتيجة لعدم وجود نصوص خاصة بالجرائم المعلوماتية في اليمن وعدم كفاية التشريعات النافذة ذات العلاقة ومنها القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية اليمني، أيضاً لعدم انطباق النصوص التقليدية عليها لكونها تدخل ضمن الأموال المعلوماتية الواقعة بواسطة تقنية المعلومات ولصعوبة التحري والإجراءات. غير أني أجد أن ما جاء في المادة (41) من (40) لسنة 2006م بالنص على أن " يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب أحكام القوانين النافذة بواسطة إستخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عل سنة أو بغرامة لا تقل عن ثلاثمائة ألف ريال ولا تزيد على مليون ريال" يمكن للقاضي أن يطبقها على كل الجرائم التي تقع باستخدام الوسائل الإلكترونية ومنها الجرائم الواقعة على النظام المعلوماتي محل دراستنا.

هذا وقد جرم مشروع القانون لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات اليمني، هذه الجريمة في المواد (13، 14، 15) منه، حيث نصت المادة (13) منه، على أنه:" يعاقب بالحبس مدة لا تقل عن شهر ولا تزيد على سنتين وبغرامة لا تقل عن مائة ألف ريال ولا تزيد على مائتي ألف ريال كل من قام عمداً بإضافة بيانات إلى نظام المعلومات الإلكتروني أو حذف أو عدل أو نسخ أو أتلف أو أخفى البيانات التي يتضمنها النظام."، وفي المادة (14) منه، فقد نصت على أنه:" يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة لا تقل عن مائة ألف ريال ولا تزيد على ثلاثمائة ألف ريال كل من تعمد ارتكاب أي فعل بوسيلة من وسائل تقنية المعلومات أدى إلى إتلاف موقع إلكتروني أو تعطيله أو إخفائه أو تغيير تصاميمه أو تعديل محتواه أو شغل عنوانه أو انتحال صفة أو شخصية مالكه."، أما المادة (15) منه، والتي نصت على أنه:" يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات أو بغرامة لا تقل عن مليون ريال ولا تزيد على ثلاثة ملايين ريال كل من تعمد ارتكاب أي فعل بأي وسيلة من وسائل تقنية المعلومات أدى إلى إعاقة أو إيقاف أو تعطيل نظام المعلومات الإلكتروني أو ألحق ضرراً بالمستخدمين أو المستفيدين.".

في حين أن مشروع القانون المعدل في سنة 2020م، بشأن قانون مكافحة جرائم تقنية المعلومات اليمني، فقد تناول هذه الجريمة في المادة (11) منه، والتي نصت على أنه:" يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مليون ريال ولا تزيد على خمسة ملايين ريال أو بإحدى هاتين العقوبتين كل من تسبب متعمداً في تعطيل شبكة معلوماتية أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجراء بدون وجه حق معالجات إلكترونية للبيانات الخاصة بها يعاقب كل من تسبب بخطئه في ذلك بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسمائة ألف ريال ولا تزيد على مليوني ريال أو بإحدى هاتين العقوبتين."، وفي

المادة (6/ب) منه، جرمت هذه الجريمة حيث نصت على أنه:" ب- فإذا ترتب على أي من الأفعال السابقة إلغاء أو حذف أو نسخ أو تغيير أو تعديل أو إتلاف أو محو أو إضافة أو تعطيل أو تخريب أو إعاقة أو توقيف أو نقل أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي، تكون العقوبة الحبس مدة لا تزيد على سنتين وبغرامة لا تزيد على ثمانية مليون ريال أو بإحدى هاتين العقوبتين."، وأيضاً في المادة (27/ب، 30/ب) منه، الخاصة بجرائم المعلوماتية ضد الدولة والسلامة العامة، حيث نصت المادة (27/ب) على أنه:" ب- إذا ترتب على أي من الأفعال السابقة إلغاء أو حذف أو نسخ أو تغيير أو تعديل أو إتلاف أو محو أو إخفاء أو إضافة أو تعطيل في موقع إلكتروني أو في نظام معلومات إلكتروني أو شبكة معلوماتية أو وسيلة تقنية معلومات بموقع له صلة بالدولة أو أحد الأشخاص الاعتبارية أو ترتب على أي فعل من الأفعال السابقة الحصول على بيانات أو معلومات حكومية سرية، فتكون العقوبة هي الحبس الذي لا يقل مدته عن ثلاث سنوات ولا تزيد على عشر سنوات وبغرامة لا تقل عن خمسة ملايين ريال ولا تزيد على عشرين مليون ريال أو بإحدى هاتين العقوبتين."، أما المادة (30/ب) فقد نصت على أنه:" يعاقب بالحبس مدة لا تقل عن ثلاث سنوات ولا تزيد على عشر سنوات وبغرامة لا تقل عن خمسة ملايين ريال ولا تزيد على خمسين مليون ريال أو بإحدى هاتين العقوبتين كل من قام بأي عمل إرهابي على أنظمة المعلومات الإلكترونية العامة أو البيانات والبرامج المخزنة بها المتعلقة بالاقتصاد الوطني أو الأمن الوطني إذا ترتب على ذلك إتلافها أو تعطيلها أو إعاقة نشاطها، ويندرج ضمن ذلك الابتزاز والتهديد بالاختراق والتدمير لأنظمة المعلومات الإلكترونية.".

بخلاف نضيره المصري فقد عالج ذلك في القانون الخاص بشأن مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018م، في جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية المادة (١٧)، وكذلك في جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة في المادة (18)، وجريمة الاعتداء على تصميم موقع مادة (19)، وجريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة في المادة (20)، وذلك كله كان في الجزء المتعلق بالجرائم السابقة في صورتها المشددة.

وخلاصة القول، إن التشريعات الجنائية اليمنية النافذة غير كافية لمواجهة تلك الجرائم، وحتى القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية يعاني من قصور تشريعي جسيم في عدم تناول تلك الجرائم في نصوصه، وبذلك ندعو إلى إجراء التعديلات اللازمة على التشريع الجنائي اليمني والقوانين ذات العلاقة ومنها القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، والعمل على سرعة سن مشروع القانون بشأن مكافحة جرائم تقنية المعلومات لسنة 2020م لمواجهة الجرائم المعلوماتية وحتى لا يفلت الجناة في تلك الجرائم من العقاب.

المبحث الثاني: المواجهة الإدارية للجريمة المعلوماتية الواقعة على النظام المعلوماتي

تمهيد وتقسيم:

المواجهة الإدارية والقضائية للجرائم المعلوماتية تقتضي وجود المرجعية القانونية لتلك المواجهة، بالإضافة إلى وجود الخبرات التقنية لدى السلطات المختصة بنفاذ القانون، ولذلك سيتحتم علينا تناول تلك المواجهة على المستوى الدولي والوطني وذلك للاستفادة من التجارب الدولية للتطبيق في أرض الواقع على المستوى الوطني، وبناء عليه سنقسم هذا البحث إلى مطلبين.

المطلب الأول: المواجهة الدولية للجريمة الإلكترونية

بعد التطور المستمر لشبكة الإنترنت واتساع نطاقها ليشمل جميع أنحاء المعمورة، وبسبب ارتباط العالم مع بعضها البعض كقرية واحدة، أدى ذلك لظهور الجرائم المعلوماتية، والتي دائما ما يكون مرتكبها مقيم في دولة والأثر الذي يحدثه في دولة أخرى، كما أن كافة الدول تسعى إلى مكافحة تلك الجرائم بشتى الطرق، ومن أجل ذلك برزت العديد من الجهود الدولية منها على المستوى الدولي ومنها على المستوى الوطني، وهذا ما سنبينه على النحو التالي:

أولاً: جهود منظمة الأمم المتحدة:

من جهود تلك المنظمة الدولية عقد العديد من المؤتمرات المعاهدات، نبينها في الآتي:

1. المؤتمر الدولي الأول لحقوق الانسان الخاص بأثر التقدم التكنولوجي على حقوق الإنسان (مؤتمر طهران ١٩٦٨م):

تبنت الجمعية العامة للأمم المتحدة توصيات هذا المؤتمر حيث تم الاعتراف بالحق في الخصوصية، وبناءً على هذه التوصيات سنت بعض دول العالم في أوروبا وآسيا وأمريكا واليابان تشريعاتها في مجال حماية الخصوصية من الاعتداء عليها ألزمت من خلالها مواقع الإنترنت المعنية بجمع المعلومات بتسجيل أغراضها وإخضاع عملياتها لرقابة الدولة **(الغزواني، ص162).**

2. المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية لسنة 2010م:

عقد المؤتمر الثاني عشر من 12 إلى 19 أبريل 2010م، بالبرازيل تحت عنوان" استراتيجيات شاملة لتحديات عالمية نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير"، وتضمن جدول أعمال المؤتمر ثمانية بنود من بينها: جرائم

الإنترنت حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها **(رميساء، 2023، ص70).**

3. المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية لسنة 2015م:

عقد منظمة الأمم المتحدة المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أبريل 2015م، بدولة قطر وكان الموضوع الرئيسي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي ومشاركة وقررت الجمعية العامة قرارها (184/67)، النظر فيما يلي: إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة منها الجرائم الجمهور المعلوماتية **(www.un.org).**

ثانياً: جهود مجموعة الدول الثمانية (G-8) لمكافحة الجريمة الإلكترونية:

مجموعة الدول الثمانية:" هو عبارة عن منتدى سياسي حكومي أسس عام 1997م، ويضم الدول الصناعية الكبرى في العالم وهي: الولايات المتحدة الأمريكية واليابان، وألمانيا، وروسيا الاتحادية، وإيطاليا، والمملكة المتحدة، وفرنسا، وكندا، أنشأت فريق فرعي للجرائم الإلكترونية الفائقة التقنية، اعتمدت وفي الاجتماع الذي عقد في واشنطن عام ١٩٩٧م عشرة مبادئ لمكافحة جرائم الحاسوب، وكان الهدف إلا يحصل المجرم على ملاذات آمنه في أي مكان في العالم.

وتلا ذلك الاجتماع اجتماعات أخرى على مستوى وزراء العدل والداخلية لدول المجموعة الثمانية، وذلك في عام ٢٠٠٤م، وصدر البيان المشترك لهذا الاجتماع بمواصلة تعزيز القوانين المحلية لبناء القدرات العالمية لمكافحة الاستخدامات الإرهابية والإجرامية للإنترنت، وتحسين القوانين التي تجرم اساءة استخدام الجرائم الإلكترونية وسرعة التعاون في التحقيقات المتصلة بالإنترنت، واتخاذ خطوات لتشجيع اعتماد المعايير القانونية التي تتضمنها على قاعدة واسعة.

وفي بيان المجموعة في عام ٢٠٠٥م، أكدت على أن وكالات إنفاذ القانون تستجيب بسرعة لتهديدات الجريمة الإلكترونية والحوادث الخطيرة. وفي اجتماع المجموعة في موسكو عام ٢٠٠٦م، أكدت المجموعة على ضرورة اتخاذ مجموعة من التدابير لمنع الأعمال الإجرامية المحتملة في مجال الاتصالات السلكية واللاسلكية، ومنع الإرهابيين من استخدام مواقع الكمبيوتر والإنترنت لتوظيف الإرهابيين الجدد وغيرها من التوصيات، وفي اجتماع قمة دول الثمانية في سانت بطرسبرغ في ذات العام، أكدت المجموعة التزامها الجديد بالتعاون مع الشركاء الدوليين لمكافحة التهديد الإرهابي.

وفي اجتماع المجموعة في ميونخ – المانيا عام ٢٠٠٧م، اتفق الأعضاء على العمل من خلال الأطر القانونية الوطنية لتحريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية. وفي قمة المجموعة في إيطاليا عام ٢٠٠٩م، أصدرت القمة بياناً تضمن جرائم الإنترنت والأمن السيبراني، وفي قمة المجموعة في دوفيل – فرنسا عام ٢٠١١م، شددت المجموعة على أهمية الإنترنت من الناحية الاقتصادية والتعليمية والحرية والديموقراطية وحقوق الإنسان **(جلال، ٢٠١٨، ص٢١١).**

ثالثاً: المنظمة الدولية للشرطة الجنائية (الانتربول):

الانتربول: هي منظمة عالمية أنشئت في عام ١٩٢٣م، ومقرها بمدينة ليون الفرنسية، وتتكون هذه المنظمة من قوات الشرطة لأكثر من ١٨٨ دولة، وخدمات المنظمة تكمن في خدمات اتصال شرطي عالمي مأمون، وخدمات بيانات ميدانية وقواعد بيانات للشرطة، وخدمات الإسناد الشرطي الميداني، والتدريب والإنماء الشرطي، وقد أدرك الانتربول خطورة الجرائم السيبرانية منذ منتصف العقد الأخير من القرن الماضي واستضاف في عام ١٩٩٥م، المؤتمر الدولي الأول بشأن الجرائم الحاسوبية، وأنشاء المؤتمر داخل الانتربول وحدة مركزية وأربعة فرق عاملة معنية بالجرائم المتصلة بالتكنولوجيا **(الغافري، 2007، 6).** وقد عقدت عدة مؤتمرات منها: المؤتمر الثاني للجريمة الإلكترونية – سنغافورة ١-٣ أكتوبر ٢٠١٤م، تحت شعار "تحقيقات الجرائم الإلكترونية دورة كاملة وشارك فيه ممثلون السلطات إنفاذ القانون والقطاع الخاص والأوساط الاكاديمية والمنظمات الدولية من أنحاء العالم، وناقش المؤتمر تحقيقات الجرائم الإليكترونية وأحدث التقنيات المستهدفة من هذه التحقيقات بهدف تعزيز التعاون في مجالات الجريمة الإلكترونية، ومنها: الوقاية والكشف، التحقيق وتقنيات التعقب والمصادرة والطلب الشرعي، الملاحقة والمحاكمة **(البادي، 2015، ص71).**

ونظراً لاتساع نطاق الجريمة الإلكترونية وتطور الوسائل المستخدمة، واتساع شبكة الإنترنت والخصائص التي يتفرد منها هذا النوع من الجرائم بات لزاماً على اليمن أن تواكب هذه التطورات والاستفادة من المواجهة الدولية للجريمة الإلكترونية، بوضع خطوط عريضة وأساسات متينة مستفيداً من المؤتمرات والندوات الدولية المختلفة وتجارب الدول المختلفة في مواجهة الجريمة المعلوماتية، وذلك من خلال البدء من حيث أنتهى به الأخرون.

المطلب الثاني: المواجهة الوطنية للجريمة الإلكترونية

يغيب دور الدولة اليمنية في مواجهة الجرائم المعلوماتية بالشكل المطلوب، ويرجع سبب هذا الغياب إلى عدم وجود قانون خاص بمكافحة الجريمة المعلوماتية، وعدم قيام السلطة

التشريعية في سن قانون أو لائحة لمواجهة هذه الجريمة أو التصديق على مشروع القانون الذي أعدته الحكومة في عام 2018 والمعدل في عام 2020م.

وفي تقريرين صادرين عن منظمة سام للحقوق والحريات، الأول بعنوان:" ظاهرة انتحال الهوية الرقمية في اليمن الدوافع والتبعات"، والثاني:" الابتزاز الإلكتروني في اليمن الظاهرة والحل"، أوضح التقريرين غياب الدور الرسمي لمواجهة الجرائم الإلكترونية، وذلك بغياب الدور الحكومي المناط به تنفيذ إجراءات الرقابة والضبط المفترض اعتمادها لملاحقة الجريمة الإلكترونية في اليمن، فعلى الصعيد الأمني تبين أنه لا يتم التعاطي بشكل فعال مع شكاوى "الابتزاز الرقمي" وتبين للتقرير أن الإجراءات التي تعتمدها الأجهزة الأمنية بدائية وغير حاسمة في التعاطي مع هذه المشكلات بل تفتقر إلى وسائل الضبط الحديثة المتخصصة في كبح هذا النوع من الجرائم (**منظمة سام، 2023، ص16**).

أما على الصعيد الرسمي هنالك جهود تقوم بها بعض الجهات الرسمية والمتمثلة بوزارة الاتصالات وتقنية المعلومات اليمنية في صنعاء، وذلك من خلال عقد مؤتمرات وندوات بالأمن السيبراني وأمن المعلومات، وهو ما سنحاول عرضه، على النحو التالي:

أولاً: المؤتمر الوطني الأول لأمن المعلومات:

انعقد هذا المؤتمر في العاصمة اليمنية صنعاء خلال الفترة 23- 25 يونيو ٢٠١4م، والتي نظمته المؤسسة العامة للاتصالات بالتعاون مع الاتحاد الدولي للاتصالات، بمشاركة 200 من متخصصي تكنولوجيا المعلومات والمطورين ومديري أمن الشبكات من 40 شركة ومؤسسة مشاركة بهدف تطوير أمن المعلومات الوطنية، وناقش المؤتمر 12 ورقة عمل عن واقع أمن المعلومات في اليمن والتحديات الراهنة والقوانين والتشريعات السيبرانية، والجدير بالذكر أن المؤسسة تبنت مشروع مركز أمن المعلومات للاتصالات اليمنية (YT-CIRT) بناءً على توصية الاتحاد الدولي للاتصالات رقم X-1051، وخرج المؤتمر بتوصيات من أهمها ضرورة تحديث التشريعات اليمنية ذات العلاقة بأمن المعلومات وجرائم الأنترنت(**المركز الوطني للمعلومات Yemen-Nic**).

ثانيًا: المؤتمر الوطني الأول للأمن السيبراني (www.saba.ye):

انعقد هذا المؤتمر في العاصمة اليمنية صنعاء خلال الفترة ٧-٩ يونيو ٢٠٢١م، تحت شعار "نحو استراتيجية وطنية للأمن السيبراني"، والتي نظمتها وزارة الاتصالات وتقنية المعلومات اليمنية، وناقش المؤتمر ٢٠ ورقة عمل عن الأمن السيبراني مقدمة من جهات ومؤسسات وشركات وقطاعات وجامعات حكومية وخاصة وكذا باحثين وخبراء وأكاديميين.

وفي ختام المؤتمر، أكد المؤتمر الوطني الأول للأمن السيبراني، على أهمية إصدار قانون جرائم تقنية المعلومات، وإعداد مشروع قانون حماية البيانات العامة والشخصية. وأوصى المشاركون في ختام أعمال المؤتمر، الذي نظمته في ثلاثة أيام وزارة الاتصالات وتقنية المعلومات، بوضع خطة لبناء قدرات كوادر وطنية متخصصة في مجال الأمن السيبراني، وتأهيل العاملين في مجال تقنية المعلومات في مختلف القطاعات بما يمكنهم من الاستجابة الفورية لطوارئ التهديدات السيبرانية. ودعت التوصيات إلى فتح المسارات الأكاديمية للتخصص النوعي في مجال الأمن السيبراني وتطوير المناهج في التخصصات ذات العلاقة لتتضمن مواد الأمن السيبراني. وشددت على نشر الوعي لدى الأفراد والمستخدمين في مجال الأمن السيبراني من خلال حملات التوعية بالاستخدام الأمن ومخاطر جرائم الأمن السيبراني وتضمين المناهج التربوية الأساسية والثانوية مواداً عن الأمن السيبراني. وأشارت توصيات المؤتمر إلى أهمية تعزيز الشراكة في مجال الأمن السيبراني بين القطاعين العام والخاص، والتنسيق والتعاون مع الجهات الإقليمية والدولية المعنية بأمن الفضاء السيبراني بما يحفظ استقلال الجمهورية اليمنية. كما دعت إلى بحث ودراسة الانضمام إلى الاتفاقيات والمعاهدات العربية والدولية في مجال حماية البيانات والمعلومات الشخصية والتصدي لجرائم الإرهاب الإلكتروني. وأكدت التوصيات ضرورة مشاركة الجمهورية اليمنية في المؤتمرات والندوات وورش العمل الإقليمية والدولية للاستفادة من الخبرات والتجارب المختلفة في مجال الأمن السيبراني، واعتماد المحاور الرئيسية لمشروع الاستراتيجية الوطنية للأمن السيبراني. وتشكيل فرق استجابة سريعة لحوادث الأمن السيبراني لدى الجهات المعنية بالبنية التحتية الحيوية بإشراف فريق حكومي متخصص من الجهات الرئيسية ذات العلاقة بالأمن السيبراني كنواة لإنشاء المركز الوطني للأمن السيبراني. وشددت التوصيات، على أهمية سن سياسات ولوائح تنظيمية تتعلق باستضافة المواقع والخدمات الإلكترونية الحكومية وتشجيع الاستثمار في مجال تزويد واستضافة المحتوى الإلكتروني الوطني وضرورة انعقاد المؤتمر الوطني للأمن السيبراني بصفة دورية كل عام. وبناءً على ما سبق كان من الأجدر على وزارة الاتصالات التوصية بضرورة الإسراع في سن التشريعات الخاصة بتقنية المعلومات أسوة بالتشريعات العربية ومنها التشريع المصري.

ثالثاً: مشروع الاستراتيجية الوطنية للأمن السيبراني:

ناقش الاجتماع المنعقد في العاصمة اليمنية صنعاء بتاريخ 2022/4/10م، والذي ضم كلاً من وزير الاتصالات وتقنية المعلومات اليمني، ووزير العدل، ووزير الشؤون القانونية، مشروع الاستراتيجية الوطنية للأمن السيبراني المرفوع من

اللجنة المشتركة من الجهات ذات العلاقة والمكلفة بإعداد الاستراتيجية.

والذي أكد على أهمية الأمن السيبراني والذي يعد ضرورة حتمية في ظل توجهات الدولة لأتمتة الخدمات والأعمال والقيام بالربط الشبكي بين مختلف الجهات الحكومية والخاصة، وعلى أهمية مشروع الأمن السيبراني لتأمين التعاملات الإلكترونية والربط الشبكي والأتمتة ومكافحة الجريمة الالكترونية، وأكد أيضاً وعلى أهمية تضافر جهود جميع الجهات الحكومية في سبيل تعزيز الأمن السيبراني وإنجاح المشروع، وضرورة إصدار التشريعات المنظمة للأمن السيبراني ومكافحة الجرائم السيبرانية، وعلى أهمية مشاركة الوزارات ذات العلاقة في توصيف المناهج الخاصة بالأقسام الجديدة، وذلك لتدريسها في الجامعات، والتي تخص الأمن السيبراني وضرورة مشاركة مندوبي تلك الجهات في تحديد متطلبات سوق العمل من الخريجين، وأشار الاجتماع إلى توجهات الحكومة للتحول التدريجي إلى الحكومة الإلكترونية، والذي يتطلب وجود استراتيجية وطنية للأمن السيبراني تشمل التدابير القانونية والتنظيمية والتقنية والتوعية وبناء القدرات وتعزيز التعاون المحلي والدولي، وإلى ضرورة تحقيق التطور في المجال الرقمي وحماية جميع الخدمات والبيانات والشبكات والمنظومات المعلوماتية والبنى التحتيّة الحيوية المرتبطة بأجهزة الدولة(www.saba.ye).

ويأتي هذا المشروع ضمن مخرجات المؤتمر الوطني الأول للأمن السيبراني الذي أقيم في عام 2021م تحت شعار نحو استراتيجية وطنية للأمن السيبراني، وقد تم تشكيل لجنة مشتركة من المختصين في الجهات ذات العلاقة لإعداد مشروع الاستراتيجية بالاسترشاد بأفضل الممارسات العربية والدولية.

رابعاً: الندوة التعريفية بوثيقة السياسات العامة لأمن المعلومات:

نظمت وزارة الاتصالات وتقنية المعلومات اليمنية، ندوة تعريفية بوثيقة السياسات العامة لأمن المعلومات، وذلك خلال الفترة ١٦-١٧ أكتوبر ٢٠٢٣م، في العاصمة اليمنية صنعاء، حيث تم التعريف بوثيقة السياسات من قبل الوزارة واستعرضوا، خلال يومين، التعريف بأمن المعلومات ومدخل السياسات، ونبذة عن المعايير الدولية لأمن المعلومات، وسياسة الأمن المادي والبيئي، وسياسة أمن التوظيف والموظفين، والتعاقد مع الأطراف الخارجية، وسياسة الامتثال، وتصنيف وحساسية المعلومات، كما تناولت الندوة سياسة إدارة الأصول المعلوماتية، وسياسة ضبط التغيير، وخصوصية البيانات، وتطوير وصيانة الأنظمة والتطبيقات، وأمن الشبكات والأنترنت، وأمن البريد الإلكتروني، وسياسة التشفير، والحماية من الشفرات الخبيثة وفيروسات الأجهزة، والنسخ الاحتياطية والاستعادة في الحالة الكوارث، وسياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ، وتقييم وتدقيق المخاطر الأمنية، ومراقبة الأحداث الأمنية (www.saba.ye).

وكان الأولى أن يتم التنسيق بين وزارة الاتصالات ووزارة الداخلية لإقامة تلك الدورات واقتراح مشاريع قوانين لحمايتها، فكما نلاحظ ضعف الجهود الوطنية بخصوص مواجهة جرائم الأنترنت، وإن وجدت فلا ترقى إلى مستوى خطورة هذا النوع من الجرائم وخصائصها، إذ لابد أن تسارع الجهات المختصة والتشريعية في إصدار قانون خاص بمكافحة جرائم تقنية المعلومات، وكذلك قانون حماية للبيانات الشخصية والعامة، وتطوير القدرات والكوادر في هذا الجانب، ونشر الوعي المجتمعي بهذا الشأن.

المبحث الثالث: المواجهة القضائية للجريمة المعلوماتية الواقعة على النظام المعلوماتي

تمهيد وتقسيم:

سنتناول المواجهة القضائية للجريمة المعلوماتية الواقعة على النظام المعلوماتي من خلال استعراض التعاون القضائي الدولي وتسليم المجرمين، ثم نبين واقع المواجهة القضائية لتلك الجرائم على المستوى الوطني في المطالب الأتية.

المطلب الأول: التعاون القضائي الدولي

تأتى أهمية التعاون القضائي في مجال مكافحة الإجرام المعلوماتي، بسبب وجود العديد من الصعوبات التي لها علاقة بتلك الجرائم ومنها صعوبة تحديد هوية مرتكبي هذا النوع من الجرائم، وصعوبة إثباتها ونسبتها إلى مرتكبها، في ظل عالميتها وتخطيها للحدود فيما بين الدول، وكذلك المشكلات المتعلقة في كيفية استيراد البيانات التي تم تخزينها عن بعد في حالة اعتبارها دليل إثبات، حيث لا توجد قاعدة عامة لحل هذه المشكلة، دون تعاون أو مساعدة قضائية. كما أن القرارات التي تصدر من المحاكم بالنسبة لهذه الجرائم لا يمكن فرضها على دول أخرى غير التي صدرت بها، ولا يترتب عليها أي أثر قانوني ما لم تعترف بها الدول الأخرى. وكل تلك التحديات بحاجة إلى المساعدة الدولية لمواجهة تلك الجرائم، وبالتالي تعرف المساعدة القضائية الدولية بأنها:" كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم" (**الغافري، 2004، 11**).

ويكمن التعاون القضائي الدولي من الجانب الجنائي وفي مجال الجرائم المعلوماتية من جهة، أو من خلال تدريب أعضاء السلطة القضائية على مكافحة تلك الجريمة، وذلك على النحو التالي:

أولاً: التعاون القضائي الدولي من الناحية الجنائية:

أ. **صور المساعدة القضائية الدولية:** للتعاون القضائي في المجال الجنائي عدة صور منها:

1. **تبادل المعلومات:** ويشمل هذا الإجراء تقديم المعلومات والبيانات والوثائق التي لها علاقة بالاستدلال، أو التحقيق للسلطة القضائية الأجنبية، أثناء نظرها لجريمة ما، وقد تضمنت هذه الصورة العديد من الاتفاقيات الدولية، أهمها معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، كما يوجد لها تطبيق كذلك في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة الوطنية 2000م، وتشمل تبادل السوابق القضائية للجناة. **(غلّاب، ص449).**

2. **نقل الإجراءات:** يقصد به قيام دولة ما باتخاذ إجراءات جنائية وهي بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة متى ما توافرت شروط معينة من أهمها التجريم المزدوج، وأن تكون الإجراءات المطلوب اتخاذها مقره من قبل الدولة المطلوب منها اتخاذها، كما يشترط أن تكون الإجراءات المطلوب اتخاذها مهمة في الوصول إلى الحقيقة **(الغافري، 2004، ص449).**

3. **الإنابة القضائية الدولية:** يقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها.

وتهدف هذه الصورة إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيرها وفي العادة يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، ومن ثم يتم إرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب، إلا أن يحدث أن تشترط المعاهدات والاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية – عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلاً من الولوج إلى القنوات الدبلوماسية والتي من شأنه تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لو تم عبر تلك القنوات، ونصت المعاهدات الدولية ومنها معاهدة منظمة المؤتمر الإسلامي لعام 1999م بإمكانية تبادل المعلومات شفويا بين الجهات المعنية بالتحقيق في حالة الاستعجال**(الصغير، 2001، ص83).**

ب. **التعاون القضائي في مجال جرائم المعلوماتية:** ومن صور هذا التعاون، ما يلي:

1. **طلب الحفظ السريع للمعلومات:** تضمنت اتفاقية مجلس أوروبا للجريمة الإلكترونية، النص على سرية البيانات المخزنة في المادة (29)، حيث أجازت لكل طرف موقع عليها بأن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف، والتي ينوي الطرف طالب المساعدة أن يقدم طلباً للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة وضبط أو الحصول أو الكشف عن البيانات المخزنة في نظام المعالجة الآلية للبيانات. وفي حالة قبول الطلب المذكور، تلتزم الدولة المطلوب منها بحفظ تلك البيانات لمدة لا تقل عن ستون يوماً، حتى يتسنى للدولة طالبة الحفظ تقديم طلب القيام بالتفتيش أو الدخول بأي طريقة مماثلة وضبط أو الحصول أو الكشف عن هذه البيانات ولكن بعد تلقي هذا الطلب تستمر عملية حفظ البيانات إلى غاية النظر فيه بالرفض أم بالقبول **(جلال، 2018، ص 325).**

2. **التفتيش والضبط والكشف عن البيانات:**

تضمنت اتفاقية مجلس أوروبا للجريمة الإلكترونية النص على المساعدة المتعلقة بالدخول إلى البيانات المحفوظة في المادة (30)، حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش، أو أن يدخل بأي طريقة مشابهة، وأن يضبط أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف، والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة (29)، ويجب الاستجابة لمثل هذا الطلب بأسرع ما يمكن في الحالات الآتية: 1- إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية عرضة لمخاطر الفقد أو التعديل. -2- أن الوسائل والاتفاقات والتشريعات الواردة في الفقرة 2 تستلزم تعاوناً سريعاً **(www.unodc.org).**

3. **الدخول وجمع البيانات المخزنة خارج الحدود:**

من الإجراءات الجديدة التي تضمنتها اتفاقية مجلس أوروبا للجريمة الإلكترونية السماح للدول الأطراف بالدخول للبيانات المخزنة خارج نطاق الحدود؛ بشرط أن يكون ذلك بموجب اتفاق، أو أن تكون هذه البيانات متاحة للجمهور. (www.unodc.org). فملاحقة مرتكبي تلك الجرائم، وتقديمهم للمحاكمة، وتوقيع العقاب عليهم، يستلزم في الغالب القيام بإجراءات قد تتمثل تلك الإجراءات المطلوب اتخاذها – في ظل المساعدة القضائية في معاينة مواقع الإنترنت في الخارج، أو تفتيش الوحدات الطرفية في حال الاتصال عن بعد، كذلك فقد تضمنت الاتفاقية النص على تعاون الدول الأطراف فيما بينها، لجمع البيانات في الوقت الحقيقي عن التجارة غير المشروعة، والمرتبطة باتصالات خاصة على أرضها تتم بواسطة شبكة معلومات وينظم هذا التعاون الشروط والإجراءات المنصوص عليها في القانون الداخلي، ويمنح كل طرف تلك المساعدة على الأقل بالنسبة للجرائم التي يكون جمع المعلومات بشأنها في الوقت الحقيقي متوافر في الأمور المشابهة، على المستوى المحلي.

4. طلب الكشف السريع عن البيانات:

أكدت اتفاقية مجلس أوروبا للجريمة الإلكترونية على حق الدول الأطراف فيها من طلب الكشف السريع عن البيانات التي تم حفظها، في المادة (31)، حيث نصت على:" أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة، والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال، فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله"(www.unodc.org).

5. التقاط البيانات:

يوجد كذلك من الإجراءات الجديدة في مجال التعاون الدولي بخصوص مكافحة جرائم المعلوماتية، السماح للدول الأطراف في التقاط البيانات التي لها علاقة بمضمون الاتصالات النوعية التي تتم عن طريق إحدى شبكات المعلومات.

أما القانون اليمني فلم يتضمن نصوص مستحدثة تتضمن التعاون القضائي الدولي في مكافحة جرائم المعلوماتية، واقتصر الأمر على النصوص التقليدية الخاصة بالإنابة القضائية، والتي بمقتضاها يجوز للنيابة العامة أو المحكمة أثناء نظر الدعوى، أن تنيب أحدى السلطات الأجنبية في اتخاذ إجراء أو أكثر من إجراءات التحقيق الابتدائي أو النهائي، وتوجه هذه الإنابة إلى وزارة الخارجية لتبليغها بالطرق الدبلوماسية، ويجوز في أحوال الاستعجال أن توجه الإنابة مباشرة إلى السلطة القضائية الأجنبية المطلوب منها القيام بالإجراء، وفي هذه الحالة يجب أن ترسل صورة من الإنابة القضائية مصحوبة بجميع الوثائق إلى وزارة الخارجية لتبليغها بالطرق الدبلوماسية، كما أن على النيابة العامة أو المحكمة أن تقبل الإنابة القضائية التي ترد إليها بالطرق الدبلوماسية من أحدى السلطات الأجنبية، ويجري تنفيذها وفقا للقواعد المقررة في القانون اليمني ولا يجوز إبلاغ نتيجة الإجراء إلى السلطات الأجنبية قبل وصول الطلب الرسمي بالطريق الدبلوماسي إذا كانت الإنابة قد وجهت مباشرة، فهذه النصوص تتضمن إجراءات لا تتسم بالسرعة التي تتطلبها مكافحة الجرائم المعلوماتية، بحيث يتم تبادل الإنابة عن طريق إجراءات رسمية تقليدية عبر وزارة الخارجية، وذلك قد يستغرق وقتا طويلا يساعد على محو اثار الجريمة أو التلاعب بها، لأنها عبارة عن أدلة ذات طبيعة معنوية سهلة الإخفاء والتلاعب، كما أن النص المتضمن عدم التقيد بالإجراءات الرسمية، بحيث يمكن قبول طلبات المساعدة القضائية عن طريق الجهات القضائية المختصة فيما بينها دون مرور تلك الطلبات عن طريق الخارجية، لم يتضمن استخدام وسائل الاتصال السريعة مثل البريد الالكتروني أو الفاكس، وبالتالي فإن على المقنن اليمني أن يحذو حذو التشريعات الحديثة والاتفاقات الدولية في مجال الوقاية من جرائم المعلوماتية ومكافحتها، وعدم إهمال ما يخص التعاون الدولي في مكافحة ذلك النوع من الإجرام والوقاية منها وفقا للمعاهدات الدولية التي انضمت إليها الجمهورية اليمنية.

ثانياً: الجهود الدولية لتدريب أعضاء السلطة القضائية: ومن هذه الجهود، ما يلي:

1. **ورشة عمل دولية حول التدريب القضائي بشأن الجريمة الإلكترونية والأدلة الإلكترونية:**

عُقدت هذه الورشة في بوخاريست – رومانيا خلال الفترة من2 – 3يونيو2014م بمشاركة منظمة جالكسي للتكنولوجيا (GLACY) وبالمشاركة مع مجموعة الدول الأوروبية الشرقية، وقد تبنى مجلس أوروبا مفهوماً لتدريب القضاة وأعضاء النيابة العامة في مجال الجريمة المعلوماتية، وتم اختيار هذا المفهوم في جنوب شرق أوروبا وقد جرى تطوير عدد من مواد التدريب وذلك بعقد دورات أساسية وأخرى متقدمة ودورات في الأدلة الإلكترونية، وكان الهدف من ورشة العمل دعم تأصيل هذا المفهوم في دورات تدريب القضاة المحلية في الدول المستفيدة من التدريب تحت رعاية شراكة دول شرق أوروبا لمكافحة الجريمة الإلكترونية **(البادي وآخرون، ص 73).**

2. **ورشة عمل دولية في استراتيجيات تدريب أعضاء سلطات تنفيذ القانون:** عقدت في لاهاي – هولندا 12 – 16/مايو/2014م، وخُصصت هذه الورشة لممثلي معاهد التدريب التابعة لأجهزة الادعاء العام المختصة في مكافحة الجريمة المعلوماتية، وهدفت الورشة إلى تطوير الاستراتيجيات المحلية لتدريب منسوبي سلطات إنفاذ القانون أي سلطات الضبط والتحقيق والمحاكمة، وتمكينهم من الحصول على مواد التدريب التي تم تطويرها بواسطة المجموعة الأوروبية للجريمة الإلكترونية للتدريب والتعليم(www.unodc.org).

وبذلك فإن أبرز الصعوبات التي توجد في الجريمة الإلكترونية، هي تحديد هوية مرتكبها، وصعوبة إثباتها ونسبتها إلى مرتكبها، وذلك لعالميتها واتساع نطاقها وتجاوزها للحدود، فعلى المقنن اليمني والجهات المختصة في السلطة القضائية الاستفادة من التعاون الدولي القضائي، بكافة المجالات مع عدم الاخلال بحق السيادة الوطنية، والاستفادة أيضاً من الدورات وورش العمل الدولية والتي تهدف لتدريب أعضاء السلطة القضائية على مواجهة الجريمة الإلكترونية، وكذا عقد الدورات التأديبية لمأموري الضبط القضائية لتأهيلهم في مواجهة تلك الجرائم.

المطلب الثاني: المواجهة القضائية الوطنية للجريمة الإلكترونية

وسنتناول في هذا الفرع المواجهة القضائية الوطنية للجريمة الإلكترونية، وذلك أثناء مرحلة التحري وجمع الاستدلالات، ومرحلتي التحقيق والمحاكمة، وذلك على النحو التالي:

أولاً: المواجهة القضائية للجريمة الإلكترونية أثناء مرحلة التحري وجمع الاستدلالات:

تعد مرحلة التحري وجمع الاستدلالات من المراحل الهامة في بناء الدعوى الجنائية، وتقوم مهمة التحري وجمع الاستدلالات على استقصاء الجرائم وتعقب مرتكبيها، ويكون لهم في سبيل ذلك جمع كافة العناصر والقرائن والأدلة التي تفيد التحقيق في الدعوى، من خلال الانتقال إلى مكان الواقعة لإثبات حالة الأشخاص والأشياء في مكان الواقعة أي مسرح الجريمة ورفع الآثار التي تخلفت عن الجريمة، وعملية التحري الرقمي تختلف عن التحري في الجرائم المعتادة المرتكبة بالوسائل التقليدية، حيث تتعامل مع وسائط وأجهزة رقمية وأدلة غير ملموسة (**آل ثنيان، 2012، ص 53**).

ويكون من مهام أجهزة التحري تحديد من قام باختراق النظام المعلوماتي، وكيف تم هذا الاختراق، ومدى الأضرار الناجمة عنه، وفقاً لمعايير عملية يقوم بها فريق فني متخصص لجمع ومسح الأدلة، وتبدو تلك الأهمية أكثر إلحاحاً في ظل اقتراف تلك الجرائم بأساليب تقنية حديثة، وذلك ما يجعل إجراءات مرحلة جمع الاستدلالات بشكلها التقليدي لا تفي بمواجهة تلك الجرائم إجرائياً، وقد تحتاج إلى قواعد إجرائية، تتناسب مع حداثة الجريمة وتتغلب على المشكلات التي تثيرها هذه الجرائم في مرحلة التحري والاستدلال، وذلك من خلال تعاملها مع هذا النوع من الجرائم وفقاً للقواعد الإجرائية، ومن أبرز هذه المشكلات مشكلة التعامل مع البلاغات والشكاوى عبر الإنترنت، من حيث جهالتها، والشروط القانونية لكلاً منهما، ومسؤولية مأمور الضبط بشأن ذلك، وأيضاً مشكلة الاختصاص المكاني لمأموري الضبط بخصوص الجرائم الإلكترونية، وما يترتب على عدم الالتزام به من آثار قانونية قد تصل إلى البطلان عند تجاوزها، وذلك في حالة عدم وجود استثناء وارد في القانون، لكون الجريمة المعلوماتية تتسم بالاتساع وتتجاوز الحدود وتحتاج في متابعتها وكشفها تعدي تلك الحدود في العالم الرقمي، وأيضاً صعوبة كشف الجريمة وتجميع الأدلة غير المرئية، والوصول إليها يعد من أبرز المشكلات التي تواجهها جهات التحري وجمع الاستدلالات في سائر مجالات التخزين والمعالجة الآلية للبيانات (**غلاب، ص257**)، وخاصة أن المقنن اليمني لم يتضمن نصوصاً قانونية بخصوص ذلك سواءً من الناحية الموضوعية أو الإجرائية، حتى يسهل تعقب الأدلة الرقمية وجمعها والكشف عنها، ولصعوبة المعاينة ونقص الخبرات في الحفاظ على الدليل الإلكتروني والتعامل معه، وتزداد تلك الصعوبة كون المختصين من مأموري الضبط القضائي المكلفين بتحرير محاضر المعاينة قد لا تتوافر لديهم الخبرات الفنية في مواجهة تلك النوع من الجرائم.

وعلى ذات الخلفية ونظراً لعدم وجود تشريع خاص لمكافحة الجريمة المعلوماتية، غير أن وزارة الداخلية ممثلة بالإدارة العامة للبحث الجنائي قامت بإنشاء إدارة خاصة لمكافحة الجرائم الإلكترونية، تختص بضبط الأنشطة غير المشروعة والتي تتم عبر شبكات الإنترنت ومنصات التواصل الاجتماعي أو تستهدف النظام المعلوماتي الخاص بالدولة أو القطاع الخاص، كما أن هذه الإدارة تتعاون مع كافة أجهزة ومؤسسات الدولة في تحديث معلوماتها لمساعدة الضباط العاملين بالإدارة، وإمدادهم بكافة الوسائل التقنية لمواجهة الجرائم المعلوماتية (**موقع الإعلام الأمني اليمني**).

وقد كشفت وزارة الداخلية عبر المتحدث الرسمي لها، إحصائية للإنجازات الأمنية للإدارة العامة للبحث الجنائي وفروعها في المحافظات، خلال فترة النصف الأول من العام 1444هـ، حيث أوضحت الإحصائية وفي سياق مكافحة الجرائم الإلكترونية، فقد تم ضبط 39 جريمة تنوعت بين تهديد وابتزاز إلكتروني وعمليات نصب واحتيال وانتحال شخصيات واختراق الكتروني وتشويه سمعة وغيرها، وقد أحيل المتهمين فيها إلى النيابة العامة، وفي آخر إحصائية للوزارة الصادرة في 12رمضان1445هـ، حيث ذكرت الإحصائية أن إدارة مكافحة الجرائم الإلكترونية في الإدارة العامة للبحث الجنائي أنجزت 17 قضية وقد أحيلت جميعها للنيابة وجهات أخرى، فيما لا تزال سبع قضايا رهن الإجراءات(**موقع الإعلام الأمني اليمني**).

ثانياً: المواجهة القضائية للجريمة الإلكترونية أثناء مرحلة التحقيق والمحاكمة:

تسمى مرحلة التحقيق التي تعرف بأنها:" مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة" (**شجاع، 2019، ص294**). ويمثل التحقيق الابتدائي المرحلة الأولى للدعوى الجنائية وهي المرحلة التي تسبق المحاكمة والتي تعد من اختصاص النيابة العامة، وقد وصف التحقيق بأنه ابتدائي لأن غايته ليست كافية فيه وإنما يستهدف التمهيد لمرحلة المحاكمة، وليس من شأنه الفصل في الدعوى بالإدانة أو البراءة، وتختلف مرحلة التحقيق عن مرحلة جمع الاستدلالات، وذلك في أن مرحلة التحقيق تعد أشد خطورة من مرحلة جمع الاستدلالات، وذلك لأنها قد تمس حقوق وحريات الأفراد، كونها تقوم على إجراءات التفتيش والضبط والقبض ثم إعداد قرار الاتهام الذي يمثل الإذن

بتحريك الدعوى الجنائية حيال المتهم، ونظراً لخطورتها حرصت معظم الدول على وضع تشريعات خاصة بتلك الجرائم ومنها المعلوماتية كضمانات تكفل حماية حقوق الخصوم، وبالتالي فمرحلة التحقيق في الجرائم التقليدية تختلف عن مرحلة التحقيق في الجرائم المعلوماتية، لأن الإجراءات المطلوبة اتخاذها في الجرائم المعلوماتية تواجهها العديد من المشاكل التي قد تعيق القيام بها أذ أنها ذات طابع تقني يحتاج إلى الاستعانة بالخبرات الفنية، تقوم بتفتيش مكونات الحاسب الآلي وكشف غموض الجريمة وتجميع أدلتها لمساعدة المحقق في أثبات الجريمة المعلوماتية(**أل ثنيان، 2012،ص 63**). أما مرحلة المحاكمة والتي يطلق عليها مرحلة التحقيق النهائي، فمن المشاكل التي تتعلق بهذه المرحلة، هي مشكلة الاختصاص القضائي، ومشكلة الإثبات بالدليل الرقمي – حجية الدليل الرقمي – سواءً كانت متعلقة بطبيعة الدليل ذاته، أو إلى حجيته في الإثبات (**غلاب، 2011، ص374**).

وتأسيسا على ما سبق، يصح القول إن الإجراءات التي تتخذها النيابة العامة أو المحكمة في نظر الجرائم المعلوماتية في مرحلتي التحقيق والمحاكمة تتم وفقاً للقواعد العامة في قانون الجرائم والعقوبات والإجراءات الجزائية، وذلك لعدم وجود تشريع خاص لمكافحة تلك الجرائم، ومن السبل التي تتم لمواجهة تلك الجرائم قامت به وزارة العدل اليمنية، ونقابة المحامين اليمنيين، بعقد دورات تدريبية متخصصة، لتدريب القضاة وأعضاء النيابة العامة والمحامين، وذلك كما يلي:

1) الدورة التدريبية حول الدليل الإلكتروني:

أقامت الإدارة العامة للتدريب والتأهيل بوزارة العدل اليمنية في صنعاء، خلال الفترة من 9 – 10 فبراير 2021م، وبالتنسيق مع هيئة التفتيش القضائي اليمنية، في العاصمة اليمنية صنعاء، دورة تدريبية حول الأدلة الإلكترونية، والتي ضمت عشرين قاضياً من قضاة المحاكم بأمانة العاصمة، وتهدف الدورة إلى أهمية تنمية مهارات القضاة المشاركين في الدورة وإكسابهم معارف ومعلومات عن الوضع القانوني للمعاملات الإلكترونية، ورفع أداء القضاة في مختلف المجالات الاليكترونية، خاصة القضاة العاملين في الميدان بما يخدم العملية القضائية ورفع مستوى الإنجاز، وتنمية قدرات القضاة حول كيفية التعامل مع الجرائم المعلوماتية بمعرفة تقنية، ومساعدة رجال الضبط القضائي وسلطات التحقيق لإثبات الحقيقة بطرق علمية وأدلة الإلكترونية، وذلك لأن المعرفة التقنية أصبحت ضرورة لمعرفة التعامل مع الجرائم الإلكترونية التي من الصعب إثباتها لعدم تناسب النصوص المنظمة لطرق الإثبات التقليدية مع طبيعة الجريمة الاليكترونية، ما يتطلب تبني الأدلة الإلكترونية التي تُعرف بأنها معلومات مخزنة ومنتقلة يمكن الاعتماد عليها في المحكمة (**موقع وزارة العدل اليمنية**).

كما هدفت الدورة إلى تعزيز وتنمية قدرات قضاة المحاكم التجارية والأموال العامة والجزائية والضرائب والمرور ومحاكم أمانة العاصمة في الدليل الجنائي وإكسابهم مهارات تقنية لمواكبة التطور الإلكتروني والاستفادة منه في مكافحة الجرائم الإلكترونية.

في حين ركزت الدورة على محاور تتعلق بالجوانب التقنية والفنية والمعاملات الإلكترونية وصورها في الواقع العملي وطبيعة الوضع القانوني لها والموقف التشريعي منها وطرق وأنماط وصور الإثبات الإلكتروني، والصعوبات في التطبيق العملي والحلول والمعالجات الخاصة بها.

2) الدورة التدريبية المتخصصة بالجريمة الإلكترونية وأنظمة الدفع المالية والمصرفية والإلكترونية: أقام مركز التأهيل والتدريب بنقابة المحامين اليمنيين بصنعاء، الدورة التدريبية المتخصصة بالجريمة الإلكترونية وأنظمة الدفع المالية والمصرفية والإلكترونية المنعقدة في صنعاء، بتاريخ 21 فبراير 2024م، بالتعاون مع وزارة العدل اليمنية، والتي شارك فيها 100 من أصحاب الفضيلة القضاة وأعضاء النيابة العامة والمحامين اليمنيين (**www.moj.gov.ye**).

وخرجت الدورة بعدد من التوصيات أهمها:

1- إنشاء نيابة ومحكمة متخصصة بالجرائم الإلكترونية وتعزيزها بكادر فني متخصص في هذا الجانب وتكون النواة الأولى للإنشاء في أمانة العاصمة.

2- التوعية العامة بأهمية تعلم الحماية من الجرائم الالكترونية.

3- العمل على مناقشة وإثراء قانون جرائم تقنية المعلومات من قبل المختصين والخبراء والمعنيين قبل إصداره.

4- إنشاء وحدة تعنى بالجرائم الإلكترونية تتبع مكتب النائب العام.

5- الاستمرار في تأهيل القضاة وأعضاء النيابة العامة وتدريبهم في هذا المجال.

6- الاستفادة من التجارب العربية التي سبقتنا في هذا المجال.

7- إضافة مواد معينة ترتبط أساساً بالدليل الإلكتروني وإلى قانون الإثبات ويعتبر قاعدة أو ضابطاً أو معياراً يستند إليه ونص بقانون العقوبات بشأن الجريمة الإلكترونية.

المبحث الرابع: الرؤية المقترحة لمواجهة الجريمة المعلوماتية الواقعة على النظام المعلوماتي

تمهيد وتقسيم: سنتأول في هذا المبحث الرؤية المقترحة لمواجهة الجريمة المعلوماتية الواقعة على النظام المعلوماتي من خلال المواجهة التشريعية للجريمة المعلوماتية وكذلك المواجهة التقنية لتلك الجريمة وذلك في المطلبين الآتيين.

المطلب الأول: المواجهة التشريعية للجريمة المعلوماتية

من المعلوم أن القانون الجنائي يقوم على مبدأ الشرعية الجنائية التي تعد من المبادئ الأساسية في القانون الجنائي، ولا يمكن تقرير أي سلوك جنائي بأنه مجرم أو أن تقرر له عقوبة إلا بناء على نص قانوني. وبناءً على ما سبق سنتناول أهم التشريعات اليمنية التي نواجه الجرائم المعلوماتية من خلالها.

أولاً: القرار الجمهوري بالقانون رقم (12) لسنة 1994م، بشأن الجرائم والعقوبات اليمني:

من المعلوم أنه لا يوجد قانون خاص لمكافحة الجريمة المعلوماتية في الجمهورية اليمنية، وبذلك يتم التعامل مع تلك الجرائم من خلال تطبيق أحكام قانون الجرائم والعقوبات، ذلك القانون الذي يحتاج إلى التعديلات اللازمة من أجل مواجهة الجرائم المستحدثة ومنها الجرائم الواقعة على النظام المعلوماتي.

ثانياً: القانون رقم (19) لسنة 1994م، بشأن الحقوق الفكرية:

نظم في مواد الباب الأول منه حق المؤلف الفردي في الفصل الأول منه في المواد (1 إلى 28)، وتناول في الفصل الثاني منه العمل الفكري الجماعي في المواد (29 إلى 43)، وكذلك نظم الحق في براءات الاختراع والاكتشاف في الباب الثاني في المواد (49 إلى 57)، وتناول في الباب الثالث حق المخترع في المواد (68 إلى 84) ويقرر في الباب الرابع الأحكام العامة والختامية والعقوبة المقررة للاعتداءات التي قد تقع على الحقوق الواردة في هذا القانون.

غير أن ذلك القانون ورغم إضافة قوانين أخرى خاصة بالحقوق الفكرية ومنها القانون رقم (15) لسنة2012م بشأن حق المؤلف والحقوق المجاورة إلا أن ذلك القانون لم يتناول الجرائم المعلوماتية وندعو إلى إجراء التعديلات اللازمة عليه وإضافة النصوص التي تجرم المساس بالحقوق الفكرية الرقمية وتعاقب عليها.

رابعاً: القانون رقم (2) لسنة 2011م، بشأن براءة الاختراع ونماذج المنفعة وتصميم الدوائر المتكاملة والمعلومات غير المفصح عنها:

حرصاً من قبل المقنن اليمني توفير أكبر قد من الحماية القانونية لنظام المعلومات، سن القانون رقم (2) لسنة 2011م، بشأن براءة الاختراع ونماذج المنفعة وتصميم الدوائر المتكاملة والمعلومات غير المفصح عنها اليمني، والذي تم تقسيمه إلى سبعة أبواب، تناول في الباب الأول منه التسمية والتعاريف والأهداف، أما الباب الثاني تحت عنوان براءة الاختراع ونماذج المنفعة، وتناول في الباب الثالث منه تصميمات الدائر المتكاملة، في حين بين الباب الرابع المعلومات غير المفصح عنها، وفي الباب الخامس تناول التراخيص الإجبارية، وتضمن الباب السادس العقوبات، والسابع منه تضمن الأحكام العامة والختامية، وذلك كله في 48 مادة. غير أن هذا القانون لم يتناول الجرائم المعلوماتية الواقعة على النظام المعلوماتي بصورة متكاملة.

خامساً: القانون رقم (40) لسنة 2006م، بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية:

تناول وسائل الحماية في الفصل الثامن منه الخاص بالعقوبات، في المادة (38)، والذي نص على أنه:" يعاقب كل من قام بإنشاء أو نشر أو تقديم شهادة توثيق مستعيناً، بطرق احتيالية بغرض الاستيلاء أو التوصل إلى الحصول على فائدة مادية له أو لغيره بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مليون ريال مع إرجاع المبالغ التي قام بالاستيلاء أو الحصول عليها أو سهل للغير الحصول عليها"، وفي المادة (41) من ذات القانون جرمت كل الجرائم التي ترتكب بالوسائل الإلكترونية بشكل عام حيث نصت على أنه:" يعاقب كل من يرتكب فعلاً يشكل جريمة بموجب أحكام القوانين النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة أو بالغرامة لا تقل عن ثلاثمائة ألف ريال ولا تزيد على مليون ريال". كما تناول هذا القانون تعريف المصطلحات المتعلقة بالبيانات والرسائل المعلوماتية، وذلك في المادة رقم (2) منه ولم يشير على الجرائم المعلوماتية.

سادساً: مشروع القانون بشأن مكافحة جرائم تقنية المعلومات:

اقترحت الحكومة اليمنية في العاصمة اليمنية صنعاء ممثلة بوزارة الشؤون القانونية إلى رئيس المجلس السياسي الأعلى في عام 2018م مشروع قانون بشأن جرائم تقنية المعلومات، وهذا المشروع يتكون من خمسة فصول، يتضمن الفصل الأول التعاريف والفصل الثاني الأهداف ونطاق السريان، والفصل الثالث أمن تقنية المعلومات، والفصل الرابع الجرائم والعقوبات، والفصل الخامس التعاون الدولي، ويتكون من 51 مادة.

وفي عام 2020م، قامت وزارة العدل اليمنية بتعديل مشروع القانون لسنة 2018م، وأقرت مشروع قانون جديد لسنة 2020م، بشأن جرائم تقنية المعلومات، ويتكون هذا المشروع من سبعة أبواب، تناول الباب الأول منه التسمية والتعاريف، وفي الباب الثاني الأهداف ونطاق السريان، وتضمن الباب الثالث الجرائم والعقوبات، أما الباب الرابع بين الأحكام العامة، والباب الخامس نظم القواعد الإجرائية، وخصص الباب السادس للتعاون الدولي، في الباب السابع بين الأحكام الختامية. وقد قدم مشروع القانون لسنة 2020م، إلى مجلس النواب لإقراره، وقامت لجنة النقل والمواصلات في اجتماعها بتاريخ 15فبراير2021م بدراسة ذلك المشروع وتوجيه مذكرات الى كل من (وزارة العدل ووزارة الداخلية وجهاز الأمن والمخابرات والنائب العام) لموافاة اللجنة بملاحظاتهم حول

مشروع القانون، وأقرت اللجنة تكليف مكتبها بالبحث عن عدد من قوانين الدول العربية بشأن قانون مكافحة جرائم تقنية المعلومات وتجهيزها خلال الأسبوع القادم حيث سيتم البدء بمناقشة مشروع القانون(**https://yemenparliament.gov.ye**).

غير أن مشروع ذلك القانون لم يرى النور إلى حين إعداد هذا البحث، وندعو البرلمان اليمني إلى ضرورة سن ذلك الموضوع مع تحديثه ليتناول كافة الجرائم الواقعة على النظام المعلوماتي، لينظم بذلك السلطات الخاصة بالتحري وجمع الاستدلالات والتحقيق، وكذلك المحاكمة والتقاضي لعدم كفاية النصوص التقليدية سواءً الموضوعية منها أو الإجرائية لمواجهة هذا النوع من الجرائم، وذلك لوجود عقبات وإشكاليات كثيرة منها إجرائية متعلقة بالضبط والتحقيق وإجراءات التقاضي، مستفيداً من التشريعات الإقليمية والدولية ذات العلاقة.

وفي جميع الأحوال ما نود التنويه إليه أن التشريعات المتعلقة بالبيئة الرقمية أو المرتبطة بها عديدة ومنها: تشريعات الملكية الفكرية التي تضم العلامات التجارية والملكية الفنية والأدبية للمصنفات الرقمية وحماية براءات الاختراع على المنتجات الرقمية. وكذلك تشريعات جرائم الكمبيوتر ومن ثم تطورها لتشمل جرائم شبكة المعلومات العالمية ضمن مفهوم أشمل هو أمن المعلومات. وتشريعات الخصوصية أو قواعد حماية تجميع ومعالجة وتخزين وتبادل البيانات الشخصية. بالإضافة إلى تشريعات المحتوى الضار الخاصة بحماية الشبكة من الدخول غير المشروع أو ما تسمى الجرائم الواقعة على النظام المعلوماتي. وكذلك تشريعات التجارة الإلكترونية التي تشمل التسوق الإلكتروني والتعاقدات الإلكترونية والتوقيع الإلكتروني. ثم تشريعات الاستثمار والتجارة والجمارك والاتصالات والضرائب والأنظمة الحكومية المرتبطة بالمشروعات التقنية ذات الصلة بتقانة المعلومات. وأيضا التشريعات المالية والمصرفية ذات الصلة بالمال الإلكتروني وتقنيات الخدمات المصرفية في بيئة الشبكة العالمية للمعلومات **(عرب، 2002، ص35)**. وبالعودة إلى مطالعة التشريعات اليمنية رغم حداثة بعضها ومنها تشريعات الملكية الفكرية إلا أنها لم تتناول حماية المصنفات والمنتجات الرقمية ضمن تشريعاتها أسوة بدول الإقليم، وقد أحسن المقنن في سن قانون 40 لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، غير أنه لم يتوسع في استيعاب كافة الجرائم المعلوماتية في نصوصه، كذلك لم يتناول النصوص ذات الصلة بالمال الإلكتروني، بينما بقية التشريعات التي سبقتنا بها معظم الدول كالجرائم الإلكترونية وأمن المعلومات، وحماية الخصوصية المتعلقة بالبيانات الشخصية والأنظمة الحكومية المرتبطة بالمشروعات التقنية ذات الصلة بتقانة المعلومات، لم يسن لها أي تشريعات ومازال القضاء وسلطة التحري والتحقيق تتعامل مع الجرائم الناتجة عنها وفقا للقواعد العامة الواردة في التشريعات اليمنية ومنها قانون الجرائم والعقوبات.

المطلب الثاني: المواجهة التقنية للجريمة المعلوماتية

أولا: تعزيز أنظمة الحماية:

مما لا شك فيه أن الحكومة اليمنية تسعى جاهدة إلى تعزيز نظام الحماية التقنية لنظامها المعلوماتي الخاص بأمنها الداخلي والخارجي وكذلك نظامها الاقتصادي من خلال تعزيز أنظمة البنوك والنظام المالي وكذلك تعزيز أنظمة الحماية في الجانب الأمني والعسكري، من خلال التدريب والتأهيل واختيار أفضل الكوادر الفنية في المجال التقني، ومن أجل ذلك تعمل أغلبية الدول في الاهتمام بجانب التدريب المتعلقة بالمجال السيبراني لكل من الموظفين المتخصصين والمكلفين بإنفاذ القانون والموظفين غير المتخصصين، حيث يتلقى الموظفون المتخصصون والمكلفون بإنفاذ القانون تدريبًا تناول مجموعة من الموضوعات بداية من التوجيه التقني وأسس التحقيقات إلى المسائل المتعلقة بجمع الأدلة الإلكترونية واستخدام أدوات التحليل في المجال المعلوماتي. وبناءً عليه نقترح على الحكومة اليمنية العمل على تأهيل الكوادر الفني في مجال الحماية من الجرائم المعلوماتية لاسيما في مرحلتي جمع الاستدلال والتحقيق **(البادي وآخرون، 2015، ص42)**.

ولتحقيق ذلك يجب على الحكومة اليمنية اتخاذ الإجراءات الأتية:

1) إصدار التشريعات المواكبة لتطورات الجريمة الإلكترونية وانسجام التشريعات الوطنية مع الاتفاقيات والقواعد الدولية والقوانين المقارنة ذات الصلة لتمكين أجهزة العدالة الجنائية من أداء دورها على النطاق الوطني والإقليمي والدولي بالصورة التي تسهم بالمكافحة الفعالة للجريمة الإلكترونية.

2) رفع كفاءة الأجهزة التقنية المختصة برصد التهديدات والمخاطر والتبليغ بالإنذار المبكر وتزويدها بأحدث المعدات.

3) تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وترشيد وتطوير أدائهم.

4) تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية.

5) إتباع كافة وسائل التوعية الأمنية للحد من مخاطر الجريمة المعلوماتية.

ثانيا: المواجهة من خلال الأمن السيبراني.

الأمن السيبراني يسمى الأمن المعلوماتي ويقصد به" مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونُهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة

وأصول المستعملين"(الاتحاد الدولي للاتصالات-- ITU tx.12.5).

وتأتي أهمية الأمن المعلوماتي نظرًا لاعتماد كافة المؤسسات المختلفة على المعلومات، لاسيما أن الاستخدامات الالكترونية في نمو وتطور مستمر نتيجة ظهور الإدارة الإلكترونية والحكومة الالكترونية والتجارة الإلكترونية والتسويق الالكتروني وكل تلك تحتاج إلى بيئة أمنة وأنظمة أمنه تتمتع بالحماية القانونية والتنظيمية (العوادي،2016، ص7). وفي ذات الإطار وبالرغم من اهتمام الجامعات اليمنية الحكومية والخاصة بفتح أقسام الأمن السيبراني ضمن كلياتها الخاصة بتقنية المعلومات لتأهيل مخرجات في هذا المجال وهذا أمرا حسن إلا أننا بحاجة إلى الإطار التشريعي والقانوني لجعل تلك المواجهة للجرائم المعلوماتية في كافة المؤسسات العامة والخاصة قانونية.

ثالثًا: المواجهة من خلال الذكاء الاصطناعي.

الذكاء الاصطناعي: "هو فرع من علوم الحاسب الآلي يتعلق بمحاكاة السلوك الذكي في أجهزة الحاسوب"(Dictionary Merriam Webster) كما يعرف بأنه" نظرية وتطوير أنظمة الحاسوب القادرة على القيام بمهام تتطلب عادة الذكاء البشري كالإدراك والتعرف على الكلام واتخاذ القرارات وترجمة اللغات"(Dictionary Oxford). ويعرف بأنه " اسم يطلق على مجموعة من الأساليب والطرق الجديدة في برمجة الأنظمة المحاسبية، التي تستخدم لتطوير أنظمة تحاكي بعض عناصر ذكاء الإنسان، وتسمح لها بالقيام باستنتاجية عن حقائق وقوانين يتم تمثيلها في ذاكرة الحاسب" (شقفه،2021، ص10). ومن المفاهيم السابقة نستنتج أن الذكاء الاصطناعي يعد نظام يقوم من خلال برمجيات وخوارزميات على الحاسب الآلي يتم تزويدها بمعلومات وتقنية قادرة على الحصول على المعلومات وتطويرها وابتكار وسائل حديثة في كافة المجالات على نحو يحاكي ذكاء الإنسان الخارق للعادة.

ويمكن الاستفادة من الذكاء الاصطناعي في مواجهة الجرائم المعلوماتية من خلال الآتي:(زروق،2024، ص51)

1- تمكين أجهزة الحاسوب من معالجة المعلومات بطرق أقرب إلى تفكير الانسان مع القدرة على حل المشاكل التي تواجهه تلك المعلومات.

2- تطوير أنظمة الحماية الإلكترونية في الحواسيب بشكل يفوق تفكير المجرم المعلوماتي بل والعمل على تحديثها باستمرار ومواجهة الجريمة فور حدوثها.

3- تطوير أنظمة الحاسوب وفقا للعقل البشري السوي من خلال البرمجة الذاتية وتطوير ملكة الابتكار والإبداع في كافة المجالات لوضع العقبات أمام التفكير المنحرف من قبل بعض البشر.

4- تطوير الخوارزميات في مجال البحث عن أفضل الحلول للمشكلات المتعلقة بالجرائم الإلكترونية ومواجهتها بشكل مباشر بل وتوقعها قبل حدوثه.

5- تطوير الأنظمة والروبوتات التي تستشعر الإعمال الإجرامية الخاصة بالأنظمة المعلوماتية من أجل كشفها وكشف مجرميها.

6- العمل على سلامة الأنظمة الحكومية والخاصة من خلال تأمينها وعدم وجود ثغرات تعرضها للاختراق.

7- التنبؤ بالجريمة قبل حدوثها والعمل على إجهاضها مبكرا من خلال الكشف عن خطورة المجرم وطريقة تفكيره ووضع التدابير اللازمة لمنعه من مواصلة الجريمة أو العودة إليها (الشريف، محمد صلى الله عليه وسلم، ص محمد صلى الله عليه وسلم).

وخلاصة القول، يتحتم على حكومة الجمهورية اليمنية متابعة السلطة التشريعية للعمل على سن التشريع الخاص بتقنية المعلومات، والعمل على تدريب وتأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية وتطوير أدائهم. بالإضافة تدريب وتأهيل المختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية، والعمل على تعزيز الحماية على أمن المعلومات بالاستفادة من الذكاء الاصطناعي في تطوير وسائل تلك الحماية.

الخاتمة

بعد أن تناولنا الجريمة المعلوماتية المتعلقة بالنظام المعلوماتي ووسائل مواجهتها من الناحية الإدارية والقضائية وفق رؤية مستقبليه لتعزيز طرق الحماية من تلك الجرائم التي تستهدف أنظمة القطاع العام والخاص، وتوصلنا إلى مجموعة من النتائج والتوصيات تتمثل فيما يلي.

الاستنتاجات:

1- إن التشريعات الجنائية اليمنية النافذة غير كافية لمواجهة تلك الجرائم، رغم حداثة بعضها ومنها تشريعات الملكية الفكرية إلا أنها لم تتناول حماية المصنفات والمنتجات الرقمية ضمن تشريعاتها اسوه بدول الإقليم، وكذلك القانون 40 لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، غير أنه لم يتوسع في استيعاب كافة الجرائم المعلوماتية في نصوصه، ولم يتناول النصوص ذات الصلة بالمال الإلكتروني، بينما بقية التشريعات التي سبقتنا بها معظم الدول تناولت نصوصها الجرائم الإلكترونية وأمن المعلومات، وحماية الخصوصية المتعلقة بالبينات الشخصية والأنظمة الحكومية المرتبطة بالمشروعات التقنية ذات الصلة بتقانة المعلومات.

2- مازالت سلطات نفاذ القانون تتعامل مع الجرائم المتعلقة بالأنترنت أو النظام المعلوماتي من الناحية الموضوعية

والإجرائية وفقا للقواعد العامة الواردة في التشريعات اليمنية ومنها قانون الجرائم والعقوبات وقانون الإجراءات الجزائية تلك التي لم يدخل عليها التعديلات المطلوبة لاستيعاب تلك الجرائم المستحدثة.

3- وجود مشروع القانون بشأن مكافحة جرائم تقنية المعلومات لسنة 2018 والمعدل في سنة 2020م غير أنه مازال حبيس الأدراج ولم يسن بقانون لمواجهة الجرائم المعلوماتية المتزايدة في وقتنا الحالي.

4- تدني مستوى تأهيل الفنيين والمهندسين العاملين في مجال الأدلة الرقمية، والمختصين بأجهزة العدالة الجنائية على كيفية التعامل مع الأدلة الرقمية والقضايا المتعلقة بالجرائم المعلوماتية.

التوصيات

1- ندعو المقنن اليمني إلى إجراء التعديلات اللازمة على التشريع الجنائي اليمني والقوانين ذات العلاقة ومنها القانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية وتشريعات الملكية الفكرية لاستيعاب نصوص تجرم الأفعال المتعلقة بالجريمة المعلوماتية.

2- العمل على سرعة سن مشروع القانون بشأن مكافحة جرائم تقنية المعلومات لسنة 2020م لمواجهة الجرائم المعلوماتية وحتى لا يفلت الجناة في تلك الجرائم من العقاب.

3- إجراء التعديلات في القانون الإجرائي ليتضمن الإجراءات الواجب أتباعها أثناء جمع الاستدلال والتحقيق والمحاكمة في الجرائم المعلوماتية.

4- ضرورة سن تشريعات متعلقة بأمن المعلومات، والعمل على تعزيز الحماية لأنظمة أمن المعلومات بالاستفادة من الذكاء الاصطناعي في تطوير وسائل تلك الحماية.

المراجع:

- الكتب والمراجع العامة:

1) العوادي، أوس مجيد.2016. *الأمن المعلوماتي السيبراني*. مركز البيان للدراسات والتخطيط، العراق.

2) الصغير، جميل عبد الباقي.(2001). *الجوانب الإجرائية للجرائم المتعلقة بالأنترنت*. دار النهضة العربية، القاهرة.

3) الصغير، جميل عبد الباقي.(1992). *القانون الجنائي والتكنولوجيا الحديثة*. الكتاب الأول الجرائم الناتجة عن الحاسب الآلي، دار النهضة العربية، ط1، القاهرة، مصر.

4) إبراهيم، خالد ممدوح.(2009). *الجرائم المعلوماتية*. دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر.

5) الشوا، سامي. (1994)*ثورة المعلومات وانعكاساتها على قانون العقوبات*، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر.

6) زروق، سعاد.(2007) .*مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي الإنترنت*. دار الكتب القانونية، الجزائر.

7) شثفه، عائشة يحي. (2021) .*الحماية القانونية للمصنفات الناشئة على برامج الذكاء الاصطناعي*، رسالة ماجستير، كلية القانون، جامعة الإمارات العربية المتحدة، دبي.

8) حجازي، عبد الفتاح.(2002).*الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت*، دار الكتب القانونية، القاهرة، مصر.

9) الغزواني، نادر عبد الكريم.(د.ن). *الحماية الجنائية من جرائم الإنترنت دراسة مقارنة*. مجلة نور، بدون تاريخ نشر.

10) المومني، نهلا عبد القادر.(2010) *الجرائم المعلوماتية*. دار الثقافة، الطبعة الثانية، عمان، الأردن.

11) قوره، نائلة.(2004) . *جرائم الحاسب الاقتصادية*.ط1، دار النهضة العربية، القاهرة، مصر.

12) الزعبي، محمد وآخرون.(2002). *الحاسوب والبرمجيات الجاهزة*. دار وائل للنشر والتوزيع، ط5، عمان، الأردن.

13) أحمد، هلال عبد الله.(1997).*التزام الشاهد بالإعلام في الجرائم المعلوماتية*. دار النهضة العربية، ط1، القاهرة، مصر.

14) عرب، يونس(2002). *النظام القانوني للخصوصية الرقمية*. منشورات اتحاد المصارف العربية، الأردن.

15) المواشير، تركي بن عبد الرحمن.(2009).*النموذج الأمني لمكافحة الجرائم المعلوماتية وقياس فاعليته*، الرياض.

16) خالد ممدوح إبراهيم. (2009) .*الجرائم المعلوماتية*. دار الفكر الجامعي، ط1، الإسكندرية، مصر.

17) شجاع، محمد سيف.(2019) . *شرح قانون الإجراءات الجزائية* اليمني. مكتبة الصادق، صنعاء، الجمهورية اليمنية.

18) الشريف، محمود سلامة، (2021)، *الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي*، المجلة العربية لعلوم الإدلة الجنائية والطب الشرعي، المجلد 2، القاهرة.

الرسائل العلمية والأبحاث:

1) الزنداني، إبراهيم محمد حمود.(2019). *مقترح صياغة قانون جديد خاص بالجرائم الإلكترونية في الجمهورية اليمنية*، كلية الدراسات الإسلامية والقانون – جامعة فطاني، مملكة تايلند.

2) الجنيد، أحمد سالم محمد.(2021) *جريمة السرقة الإلكترونية*، مجلة القانون، العدد الثالث، كلية الحقوق جامعة عدن، الجمهورية اليمنية.

3) ال ثنيان، ثنيان ناصر.(2012). *إثبات الجريمة الإلكترونية*. رسالة ماجستير، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض.

4) براهيمي، جلال.(2018). *التحقيق الجنائي في الجرائم الإلكترونية*. رسالة دكتوراه، كلية الحقوق والعلوم السياسية – قسم الحقوق، جامعة مولود مغمري – تيزي وزو، الجزائر.

5) الغافري، حسين بن سعد.(2004).*الجهود الدولية في مواجهة جريمة الأنترنت*. بحث قدم إلى ندوة مكافحة الجرائم الإلكترونية، أقامتها الأمانة العامة لمجلس التعاون الخليجي.

6) حسين، خالد محمد.(2017).*الجرائم الإلكترونية*. بحث للحصول على درجة الليسانس كلية القانون، كلية القانون والعلوم السياسية، جامعة ديالي، الجزائر.

7) زروق، سعاد.(2024).*متطلبات إنجاح العدالة بين التقاضي الإلكتروني والذكاء الاصطناعي*. رسالة ماجستير، كلية الحقوق، جامعة بلحاج بوشعيب، الجزائر.
8) البادي، سعيد بن سالم وآخرون.(2016) *الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها*. مجلس التعاون لدول الخليج العربي، مسابقة الأمير نايف بن عبد العزيز للبحوث الأمنية .
9) أبكر، مصطفى سليمان.(1420) . *جرائم الحاسوب وأساليب مواجهتها*. مجلة الأمن والحياة، العدد 210، الرياض، السعودية.
10) عبد الحكيم، مولاي إبراهيم.(2015).*الجرائم الإلكترونية*. مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، العدد 23، المجلد الثاني، الجزائر.
11) رميساء، مرابط.(2023). *مواجهة الجريمة الإلكترونية ضمن تحقيق الأمن السيبراني*. ورقة بحثية، مجلة الحوكمة والقانون الاقتصادي، المجلد2، العدد2.
12) الرقيشي، محمد ناصر علي.(2018).*الإثبات الجنائي في الجريمة الإلكترونية*، رسالة ماجستير، كلية الحقوق – جامعة السلطان قابوس، عمان.
13) غلاب، فايز راجح.(2011). *الجرائم المعلوماتية في القانون الجزائري واليمني*. رسالة دكتوراه، كلية الحقوق، جامعة الجزائر.
14) رستم، هشام محمد فريد.(2019) .*الجرائم المعلوماتية- أصول التحقيق الجنائي الفني وآلية تدريب المحققين*. مجلة الأمن والقانون تعد عن أكاديمية شرطة دبي، السنة السابعة، العدد الثاني.
15) العفيفي، يوسف خليل يوسف.(2013).*الجرائم الإلكترونية في التشريع الفلسطيني دراسة تحليله مقارنة*، الجامعة الإسلامية، غزة، فلسطين.
16) نجم الدين، فيصل كامل.(2018).*واقع الجريمة الإلكترونية في مواقع التواصل الاجتماعي الحماية النظامية في دول مجلس التعاون الخليجي*، المجلة الدولية للاتصال الاجتماعي، العدد4، المجلد5، جامعة عبد الحميد بن باديس، الجزائر.

المجلات العلمية والمؤتمرات:

1) منظمة سام للحقوق والحريات.(2022) .*الابتزاز الإلكتروني في اليمن الظاهرة والحل*، مشروع الحقوق الرقمية.
2) منظمة سام للحقوق والحريات.(2023).*ظاهرة انتحال الهوية الرقمية في اليمن الدوافع والتبعات* مشروع الحقوق الرقمية – منظمة سام
3) مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين(2000).عقد المؤتمر في فيينا، في الفترة ما بين10 -17 نيسان العام2000م.

التشريعات القانونية:

1) دستور الجمهورية اليمنية لسنة 1991م وتعديلاته لسنة 2001م.
2) القرار الجمهوري رقم (12) لسنة 1994م، بشأن الجرائم والعقوبات اليمني، الصادر في 24/أكتوبر/1994م، نشر في الجريدة الرسمية العدد (19/3) لسنة 1994م.
3) قرار جمهوري بالقانون رقم (19) لسنة 1994، بشأن الحق الفكري اليمني، منشور بتاريخ 31/أكتوبر/1994م.
4) القانون رقم (40) لسنة 2006م، بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.
5) القانون رقم (175) لسنة 2018م بشأن مكافحة جرائم تقنية المعلومات المصري، المنشور في الجريدة الرسمية في العدد 32 بتاريخ 14/أغسطس/2018م.
6) القانون رقم (85) لسنة 1937م، بشأن قانون العقوبات المصري، الصادر بتاريخ 21/يوليو/1937م.
7) القانون رقم (151) لسنة 2020م، بشأن حماية البيانات الشخصية المصري، نشر في الجريدة الرسمية رقم (28) مكرر بتاريخ 13/يوليو/2020م.
8) مشروع القانون بشأن مكافحة جرائم تقنية المعلومات اليمني لسنة 2018م.
9) مشروع القانون بشأن مكافحة جرائم تقنية المعلومات اليمني لسنة 2020م.
10) قرار جمهوري بالقانون رقم (13) لسنة 1994م، بشأن الإجراءات الجزائية اليمني، الصادر بتاريخ 8/جماد الأول/1415ه، الموافق 12/أكتوبر/1994م.

المواقع الإلكترونية:

1) موقع سبأ نت، متاحة على الرابط: https://www.saba.ye ، بتاريخ ٦/يونيو/٢٠٢١م، تاريخ الدخول: ٢٠٢٤/٣/٢٢م.
2) موقع المركز الوطني المعلومات اليمني التابع لرئاسة الجمهورية، متاح على الرابط: https://yemen-nic.info/news/detail.php.، تاريخ نشر المقالة ٩/يونيو/٢٠٢١م، تاريخ الدخول ٢٠٢٤/٣/٢٢م.
3) موقع المجلس الأوربي لمكافحة الجريمة الإلكترونية، متاح على الرابط: (**www.unodc.org**)، تاريخ الدخول: 2024/4/17م.
4) موقع الأمم المتحدة على الرابط:(**www.un .org**)
5) موقع الاتحاد الدولي للاتصالات، متاح على الرابط: (**www.itu.int**)
6) موقع وزارة الاتصالات اليمنية، متاح على الرابط: (**www.unodc.org**)
7) موقع وزارة العدل اليمنية، متاح على الرابط: **(www.ptc.gov.ye).**
8) موقع مجلس النواب اليمني، متاح على الرابط: (**https://yemenparliament.gov.ye**) تاريخ الدخول 10/ 9/ 2024م.
9) موقع الإعلام الأمني، متاح على الرابط: **(www.smc.gov.ye).**