Sana'a University Journal of Human Sciences مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 4 | No. 10 | Page 185 – 221 |2025 https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

The human Right to protection from Cybercrime In international and Yemeni law

Khaled Mohammed Ali Al-Kumaim [1,*]

[1] Department of Public International Law, Faculty of Sharia and Law - Sana'a University, Sana'a, Yemen.

***Corresponding author:** *k.alkomaim@su.edu.ye*

Keywords

1. Protection
2. Information crime
3. The right to privacy
4. Personal data
5. Electronic Spy

Abstract:

Since the mid-twentieth century ،the international community has witnessed a massive information revolution due to the rapid development and scientific and technological progress in the field of information technology ،such that it has become a significant force in the hands of states and individuals. As a result of this contemporary scientific and technological progress ،criminal methods have emerged using modern technologies that have significantly impacted the issue of protecting rights and freedoms across the digital world. This technology has enabled the violation of individuals' privacy ،access to their secrets ،and their illegal exploitation. This has led to increased community interest in the right to protect the sanctity of private life at both the international and national levels.

This study outlines the nature and characteristics of cybercrimes ،the forms of cybercrimes ،and the international efforts of the United Nations to protect against cybercrimes. It then explains protection against cybercrimes in Egyptian and Yemeni law ،as well as international cooperation to combat cybercrimes (security and judicial cooperation).

The study concludes that technological developments in computers and the Internet have led to the emergence of new technologies used to violate individuals' privacy. This has also led to the emergence of new forms of crimes. Therefore ،protection against cybercrimes remains insufficient due to these technologically advanced devices ،which can accurately transmit what is happening Behind the walls.

Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 4 | No. 10 | Page 185 – 221 | 2025
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

حق الإنسان في الحماية من الجريمة المعلوماتية في القانونين الدولي واليمني

خالد محمد علي الكميم [1]*،

[1] قسم القانون الدولي العام ، كلية الشريعة والقانون - جامعة صنعاء ، صنعاء ، اليمن. .

المؤلف: *k.alkomaim@su.edu.ye*

الكلمات المفتاحية

1. حماية
2. الجريمة المعلوماتية
3. الحق في الخصوصية
4. البيانات الشخصية
5. التجسس الإلكتروني

الملخص:

شهد المجتمع الدولي منذ منتصف القرن العشرين ثورة معلوماتية هائلة، بسبب التطور السريع والتقدم العلمي والتكنولوجي في مجال تكنولوجيا المعلومات، بحيث أصبحت قوة لا يستهان بها في أيدي الدول والأفراد، ونتيجة لذلك التقدم العلمي والتكنولوجي المعاصر برزت أساليب إجرامية بتقنيات حديثة أثرت بشكل كبير على مسألة حماية الحقوق والحريات عبر العالم الرقمي، حيث مكنت تلك التكنولوجيا من انتهاك خصوصية الأفراد، والاطلاع على أسرارهم واستغلالها بشكل غير قانوني؛ الأمر الذي أدى إلى زيادة اهتمام المجتمع بالحق في حماية حرمة الحياة الخاصة على المستويين: الدولي والوطني.

وقد بينت هذه الدراسة ماهية الجرائم المعلوماتية وخصائصها، وصور الجريمة المعلوماتية، ومن ثم إيضاح الجهود الدولية لمنظمة الأمم المتحدة في الحماية من الجريمة المعلوماتية، ثم بيان الحماية من الجريمة المعلوماتية في القانون اليمني والمصري، وكذا التعاون الدولي لمكافحة الجريمة المعلوماتية (التعاون الأمني والقضائي).

وتوصلت الدراسة إلى أن التطور التقني في الحاسب الآلي وشبكة الإنترنت أدى إلى نشوء تقنيات جديدة تستخدم في انتهاك خصوصية الأفراد، كما أدى ذلك إلى ظهور صور جديدة للجرائم؛ لذا تبقى الحماية من الجريمة المعلوماتية غير كافية بسبب هذه الأجهزة المتطورة تكنولوجيا، والتي تستطيع أن تنقل بدقة ما يدور خلف الجدران.

المقدمة:

يعد حق الإنسان في الحماية من الجريمة المعلوماتية ضمن حقوق الإنسان الأصيلة، ومن أهم الحقوق اللصيقة بالشخصية الإنسانية، ونظراً لهذه الأهمية فقد تم التأكيد عليه في المواثيق الدولية والتشريعات الوطنية؛ لما له من ارتباط وثيق بحياة وحرية الفرد؛ ولذا كانت الحاجة ملحة لضمانات قانونية تحمي الفرد من الثورة المعلوماتية بأدواتها المتمثلة في جهاز الحاسوب والشبكة العالمية للمعلومات، لما لهذه الأدوات من قدرة فائقة على جمع أكبر قدر من المعلومات والبيانات عن الأفراد واسترجاعها وتصنيفها وتحليلها ومعالجتها، ثم مبادلتها.

وقد أدى التوسع والتنوع في استخدام الوسائط الإلكترونية في عصر البيئة الرقمية إلى تنامي التهديدات والانتهاكات على نحو يضر بالمصالح الخاصة للأفراد؛ كانتهاك سرية الحياة الخاصة أو سرية المراسلات، أو المصالح العامة للدولة كتزوير البيانات، والمعطيات الإلكترونية، أو التجسس والقرصنة، وغيرها من الصور التي اصطلح على تسميتها بالجريمة المعلوماتية التي مهما تعددت تسمياتها، واختلف من تشريع لآخر إلا أن أثرها واحد، الأمر الذي دفع بالتشريعات الدولية والداخلية إلى البحث عن الحلول المجدية للتقليل من خطر هذه الجريمة إن لم يكن القضاء عليها نهائيًّا، مع ما تعترضها من صعوبات موضوعية وإجرائية تعكس في النهاية خصوصية مكافحة الجريمة المعلوماتية.

وقد اكتسبت جرائم الحاسب الآلي طابع الجرائم الدولية باعتبار بعضها يشكل جرائم عابرة للحدود، إلا أن ذلك لا يعني اعتبارها من قبيل الجرائم التي تنظم في القانون الدولي الجنائي، وإن تم النص على بعض قواعدها ضمن اختصاصات المحكمة الجنائية الدولية ونظامها الأساسي في روما عام 1998م[1].

وأمام ما تمثله هذه الجرائم من خطر فقد اهتم المجتمع الدولي بمسألة مكافحة الجريمة المعلوماتية، وفي مقدمة الكل منظمة الأمم المتحدة التي أولت مسألة مواجهة الجرائم المعلوماتية اهتماماً كبيراً في الكثير من الأعمال الدولية المهمّة، ولعل آخرها الخطوة التاريخية بصدور قرار الجمعية العامة للأمم المتحدة بتاريخ 24-12-2024م باعتماد اتفاقية مكافحة الجرائم المعلوماتية، وهو تطور عالمي بما يمثله من حماية لخصوصية الإنسان وضحايا الاستغلال المعلوماتي بكافة أنواعه، مع تفعيل التعاون القضائي وتبادل الأدلة الاليكترونية بين الدول.

وسوف تسعى هذه الدراسة إلى الإلمام بموضوع الجريمة المعلوماتية من خلال ضبط مدلولها وخصائصها، مع تسليط الضوء على مختلف الصعوبات والإشكالات التي تعترض سبيل مكافحتها وفق ما يتم العمل به في أغلب

(1) الجريمة الدولية، وفق نظام روما الأساسي محددة وعلي سبيل الحصر في جرائم الحرب، جرائم العدوان، جريمة الابادة البشرية، الجرائم ضد الانسانية، ما يجعل بالضرورة التفرقة بين النوعين، فالجريمة المعلوماتية تصنف في مجال القانون الجنائي الدولي، بخلاف الجريمة الدولية التي تصنف في مجال القانون الدولي الجنائي.

التشريعات المقارنة، مع عرض بعض الحلول التي يرى الباحث بأنها مجدية وممكنة في السعي لمكافحة الجريمة المعلوماتية.

وفي إطار الجهود الوطنية ستتطرق الدراسة إلى مسار التشريعات والسياسات والأعمال التي قامت بها الجمهورية اليمنية من أجل الوقاية من الجريمة المعلوماتية، ومواكبة لما تضمنته أحكام القانون الدولي، وبالمقارنة مع قوانين بعض الدول – كالمصري – وقرارات المنظمات الدولية.

- **مشكلة الدراسة:**

تتمثل مشكلة الدراسة في أن التنامي الرهيب لمعدلات الجريمة المعلوماتية جعلنا في مواجهة مخاطر وتهديدات تؤثر على مفهوم الحماية، وهذا ما يستوجب تطوير أنظمة معلومات وبرامج حماية للكَمِّ الهائل من المعلومات المتاحة على الإنترنت، أو التي تنشأ في البيئة الافتراضية، مع ضرورة أن تكون متاحة دون المساس بحرية الوصول إلى المعلومات، ومن أجل الإجابة عن التساؤل الرئيس السابق؟؟؟ يمكن طرح التساؤلات الفرعية الآتية:

1) ما هي الجريمة المعلوماتية؟ وما أنواعها؟ وما طرق الحماية منها؟
2) ما مدى الحاجة إلى الحماية المعلوماتية؟ وما هي متطلباتها؟
3) ماهي تحديات عالم الفضاء السيبراني في مواجهة حماية الإنسان من الجريمة المعلوماتية؟

- **أهمية الدراسة:**

تأتي الأهمية البالغة للدراسة نتيجة الارتفاع الكبير في معدلات الجريمة المعلوماتية ذات الصلة بوسائل الإعلام الجديد، كالتجسس أو قرصنة المواقع أو التعدي على خصوصية الأفراد، أو الإرهاب الإلكتروني أو تسريب المعلومات.... الخ؛ مما يتطلب تكاتف الجهود لمواجهة هذه الجرائم العابرة للحدود، وتطوير آليات الحماية والتأمين من الجريمة المعلوماتية.

- **أهداف الدراسة:**

تهدف هذه الدراسة إلى توضيح فعالية الجهود الدولية والوطنية في تعزيز حق الإنسان في الحماية من الجريمة المعلوماتية، وأثر ذلك في الحد من هذه الجرائم التي تشهد تنامياً ملحوظاً مس الحياة الخاصة للأفراد والمؤسسات الاقتصادية وأسرار المؤسسات الحكومية؛ ممّا شكل تهديداً قوميًّا لأمن الدول والمجتمع الدولي عموماً؛ ومن ثَمَّ فإن الدراسة تستهدف الآتي:

أ – تسليط الضوء على الحق في الحماية من الجريمة المعلوماتية وبيان ماهيتها.

ب – الكشف عن مخاطر التقنيات الحديثة على الحق في الخصوصية المعلوماتية.

ج – بيان جملة الجهود الدولية وما بلغته في حماية الإنسان في مجال الجريمة المعلوماتية من خلال أعمال المنظمات الدولية العالمية والإقليمية.

د – إيضاح مدى التعاون والحماية التي وفرتها القوانين المعاصرة لهذا الموضوع الحديث.

هـ – بيان الحال للواقع الوطني في تشريعات الجمهورية اليمنية إزاء كل ما يتعلق بحماية الإنسان من الجريمة المعلوماتية، ومدى مواكبتها للأعمال الدولية المعاصرة ذات الصلة، كالتشريعات المصرية.

منهج البحث:

اعتمدت الدراسة على المنهج الوصفي والتحليلي المقارن من خلال استعراض أعمال المنظمات الدولية، وما تضمنته المواثيق والمعاهدات الدولية ذات العلاقة بالحماية من الجرائم المعلوماتية، ونصوص التقنين اليمني، ثم المقارنة مع قوانين الدول المعاصرة بهذا الخصوص، والتعليق عليها وفق ما تقتضيه كل جزئية في البحث.

خطة الدراسة:

في سبيل إنجاز هذه الدراسة، قُسمت الدراسة إلى مطلب تمهيدي تم فيه استعراض ماهية الجريمة المعلوماتية: تعريفها وخصائصها، ثم أنواعها وطرق الحماية منها، إضافة الى مبحثين: تناول الأول منها الجهود الدولية في الحماية من الجريمة المعلوماتية باستعراض دور منظمة الأمم المتحدة عموما، ثم عمل الجمعية العامة، ثم النظر في الحماية من الجرائم المعلوماتية في إطار المؤتمرات والاتفاقيات الدولية، وأوضح في المبحث الثاني الحماية الوطنية والتعاون الدولي لمكافحة الجريمة المعلوماتية.

مطلب تمهيدي: ماهية الجريمة المعلوماتية

تعدُّ الجريمة المعلوماتية من جرائم العصر الحديثة والمتطورة، بسبب التقدم التكنولوجي الرهيب غير المتوقف، ممّا خلق معه الحاجة الى الحماية من هذه الجريمة ابتداء بالتوسع في بيان مكنونها وأخطارها وصورها التي تمكنت بها من المساس بحياة الفرد والمجتمع، ثم لزوم العمل الحثيث للحد منها؛ لذا كمدخل للدراسة سأبين ماهية الجريمة المعلوماتية في فرع أول، ومن ثم نبين أنواعها وطرق الحماية منها في فرع ثان، وذلك كالآتي:

الفرع الأول: مفهوم الجريمة المعلوماتية

يقتضي التطرق للجريمة المعلوماتية التعريف بها ابتداءً، ثم بيان خصائصها، وذلك على النحو الآتي:

أولاً: تعريف الجريمة المعلوماتية([2])

- **الجريمة المعلوماتية:** عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين؛ الجريمة المعلوماتية بأنها :"هي كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية"([3]).

([2]) عرفت اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية، البيانات المعلوماتية بأنها: كل تمثيل للوقائع أو المعلومات أو المفاهيم تحت أي شكل، وتكون مهيأة للمعالجة الآلية. د. ابراهيم احمد الصعيدي،نظام التشغيل الاليكتروني للبيانات،مطبعة المعرفة،1981م، ص 13،

Recommendation of the concerning guidelines for the security of information's system was adopted by the OECD Council on, 26 November 1992.

([3]) مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين (فينا / ابريل 2000م).

- وعرف خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية (OCDE) **الجريمة المعلوماتية** بأنها: "كل سلوك غير مشروع مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها"([4]).

أما قانون الحصول على المعلومات اليمني رقم (13) لسنة 2012م فقد أورد تعريف لثلاثة مصطلحات: الأول: هو مصطلح "المعلومة" وعرفها بأنها "حقائق مدركة في الوعي تتواجد معنويًّا كقيم معرفية ومادية في شكل أرقام وأحرف ورسوم وصور وأصوات، ويتم جمعها ومعالجتها وحفظها وتبادلها بوسائط إلكترونية وورقية". والثاني: "نظام المعلومات" وعرّفها بأنها "مجموعة من العناصر البشرية والمادية والفنية والتنظيمية والمعرفية والتي تتفاعل فيما بينها وتعمل معاً لتحقيق عمليات جمع البيانات والمعلومات ومعالجتها وتحليلها وحفظها وتبادلها ونشرها على النحو الذي يفي باحتياجات المستفيدين". أما المصطلح الثالث الذي جاء به هذا القانون فهو "البيانات الشخصيّة"، وعرفها بأنها "معلومات عن فرد معيّن تتعلق بسلالة هذا الفرد، أو وضعه الاجتماعي، شرط ألا يجوز الإدلاء بالمعلومات الخاصة بهذا الفرد إلا بموافقته الصريحة أو بموافقة أحد أقاربه في حالة وفاته من الدرجة الأولى حتى الدرجة الثالثة المباشرين"([5]).

ثانياً: خصائص الجريمة المعلوماتية:

يمثل الاستخدام السيئ للتقنية الحديثة تهديداً خطيراً على خصوصية وحياة الإنسان؛ لذا يلزم الإحاطة بها، ويتضمن ذلك بيان خصائص الجرائم المعلوماتية، والتي تتمثل فيما يأتي([6]):

1) أنها جرائم عابرة للحدود (الطبيعة الدولية)؛ إذْ يلعب البعد الزمني (اختلاف المواقيت بين الدول)، والمكاني (إمكانية تنفيذ الجريمة عن بعد)، والقانوني (أي قانون يطبق) دوراً مهمًّا في تشتيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم، كما تخلف هذه الخاصية الكثير من الإشكالات القانونية في مسألة الاختصاص القضائي والتحديات التي تقترن به.

2) أنها من الجرائم الناعمة التي لا تحتاج لعنف أو جهد؛ إذْ يسهل ارتكابها (نظريًّا)؛ لكونها ذات طابع تقني.

([4]) Westin, A F , Privacy and Freedom, New York, Atheneum. (1967).

Miller, A (1971), The Assault on Privacy, Ann Arbor, University of Michigan Press.

مشار إليه لدى: د. يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل مقدمة إلى:- ندوة اخلاق المعلومات، نادي المعلومات العربي،16-17 اكتوبر 2002،عمان،الأردن

([5]) في ذلت السياق يجب الاشارة إلى ان من أسباب تفاقم الجرائم الإلكترونية في اليمن خلال السنوات الأخيرة هو غياب القوانين والعقوبات التي من شأنها الحد من هذه الجرائم، قلة الوعي الرقمي وتأمين الأجهزة والحسابات، خوف الضحية من الفضيحة المجتمعية والأسرية وتعرّضها للوم، قلّة الوعي العام حول كيفية مواجهة المبتز والتصدي لهذا النوع من الجرائم.

([6]) د. احمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، 2005م، د. محمود أحمد عبابنة , جرائم الحاسوب وأبعادها الدولية , الطبعة الأولى / الإصدار الثاني , دار الثقافة لمنشر والتوزيع , عمان, 2009م , ص 35.

3) الذكاء والخبرة لمرتكب الجريمة المعلوماتية، وسرعة تنفيذها، وقلة تكلفتها.

4) ضخامة المكاسب التي يمكن للجاني تحقيقها؛ فهي مغرية للمجرمين، وذلك مقابل خسائر الغير الباهظة إذا ما قورنت بالجريمة التقليدية.

5) صعوبة الاحتفاظ الفني بآثارها إن وجدت؛ فهي جريمة لا تترك أثرًا لها بعد ارتكابها.

6) سهولة إخفاء معالم الجريمة، وصعوبة تتبع مرتكبيها.

7) تحتاج إلى خبرة فنية لإثباتها؛ إذْ يصعب على المحقق التقليدي التعامل معها.

8) كثير من جرائم الإنترنت لا يتم الإبلاغ عنها، لعدم اكتشاف الضحية، أو خشية التشهير.

ومن الثابت – إلى الآن – أنه لا توجد وسيلة آمنة وفعالة بصورة نهائية ومؤكدة، تمكن من إخفاء آثار وهوية مستخدمي الأنترنت([7]).

الفرع الثاني أنواع الجريمة المعلوماتية وطرق الحماية منها

تتعدد الجريمة المعلوماتية بشكل متجدد، وغير قابل للحصر، وفيما يلي نستعرض أهمها، ثم نتناول طرق الحماية منها، وذلك كما يأتي:

أولاً: أنواع (صور) الجريمة المعلوماتية:

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة، وبتعدد صور الجرائم التقليدية من جهة أخرى، فإن ذلك لا يعني تناول هذا الموضوع بطريقة المدرسة التقليدية التي تتمثل في سرد الجرائم التي يتناولها قانون العقوبات؛ لأنه لا يمر مرتكب الجريمة المعلوماتية بمراحل ارتكاب الجريمة التقليدية من حيث التفكير والتخطيط والإعداد والتجهيز والانتقال والرصد والتنفيذ؛ ولذا فقد جاءت التصنيفات للجريمة المعلوماتية كالآتي([8]):

1) الجرائم الماسة بالمعلومات:

يتعلق هذا التصنيف بمحل الجريمة، وحسب هذا المعيار يحوي الجرائم التالية:

أ . الجرائم الماسة بالمعلومات الشخصية والبيانات المتصلة بالحياة الخاصة: وتشمل جرائم الاعتداء على المعلومات السرية والمحمية، والاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة، ومن

([7]) د. عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط 2، 2007م، ص 245، د.عمر أبو الفتوح الحمامي، الحماية الجنائية للمعلومات المسجلة اليكترونيا، دراسة مقارنة، دار النهضة العربية،2010م، ص 148، ومن أهم جرائم الاعتداء على الأشخاص التي تقع باستخدام شبكة الانترنت هي: جرائم السب والقذف، وجرائم الاعتداء على حرمة الحياة الخاصة، وجرائم الاستغلال الجنسي للأطفال على الانترنت.

([8]) د. سعاد قصعة، تحديات الأمن المعلوماتي في مواجهة الجريمة الإلكترونية في ظل الإعلام الجديد، مجلة المعيار مجلد: 24 عدد: 50 السنة: 2020م، قسنطينة / الجزائر، ص 382 .

ذلك أيضاً جرائم السب والقذف وإنتحال الشخصية والتهديد والابتزاز وتشويه السمعة والتشهير ([9]).

ب. الجرائم الماسة بالحواسيب: مثل جرائم الإتلاف وتشويه البيانات والمعلومات وبرامج الحاسوب، باختراق وتدمير النظم واستخدام وسيلة تقنية الفيروسات، وتقع على المؤسسات في الغالب.

2) الجرائم ضد الأموال: وهي الجرائم الواقعة على أموال أو أصول، للحصول على المال، أو جرائم التحرير والتلاعب في المعلومات المخزنة داخل نظم الحاسوب واستخدامها، وأبرزها([10]):

أ- الاستيلاء على حسابات البنوك: وذلك من خلال اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، وأيضاً سرقة البطاقات الإئتمانية، ثم الاستيلاء عليها وسرقة ما بها من أموال.

ب- الجرائم الماسة بحقوق الملكية الفكرية والأدبية وحق المؤلف: مثل جرائم قرصنة البرمجيات، التي تشمل نسخ وتقليد ونشر ما يتوفر على الشبكة من إنتاج فكري وأدبي، وأيضاً الاعتداء على العلامات التجارية وبراءة الاختراع.

3) الجرائم الماسة بأمن الدول، وأبرزها:

أ. برامج التجسس: حيث تنتشر العديد من برامج التجسس المستخدمة لأسباب سياسية، والتي تهدد أمن وسلامة الدولة؛ إذْ يقوم المجرم بزرع برنامج التجسس داخل الأنظمة المعلوماتية للمؤسسات، ومن ثم هدم أنظمة النظام والإطلاع على مخططات عسكرية أو غيرها مما يخص أمن البلاد، وهذه الجرائم تعدُّ من أخطر الجرائم المعلوماتية([11]).

ب. الجرائم الإرهابية: تعتمد المنظمات الإرهابية على استخدام وسائل الاتصال الحديثة وشبكة الإنترنت، وفق أسلوب التضليل من أجل بث ونشر معلومات مغلوطة أو كاذبة، والتي تؤدي إلى زعزعة الاستقرار وإحداث الفوضى، لتنفيذ مصالح سياسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الانتفاع بمصالح شخصية ([12]).

ثانياً: طرق الحماية من الجرائم المعلوماتية (الإلكترونية):

نظراً لخطورة هذا الجريمة المتجددة وتنوع طرقها للإضرار بالإنسان أفراداً وجماعات ودول، يتوجب تعدد طرق الحماية منها، وكبح ما أمكن من هذه الأخطار، ومن تلك الطرق ما يأتي([13]):

([9]) د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، ط 1، مكتبة الوفاء القانونية، مصر، 2011م، ص 98 .

([10]) د. محمد دروش فهيم، الجريمة وعصر العولمة: ملف لأشهر المحاكمات في مصر، النسر الذهبي للطباعة، مصر، 2000 م، ص 221.

([11]) الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مركز هردو لدعم التعبير الرقمي القاهرة 2014م : www.hrdoegypt.org / info@hrdoegypt.org، ص 21 / 22.

([12]) المستشار/ د. صالح عبدالله المرفدي (عضو المحكمة العليا) الجرائم المرتكبة على وسائل التواصل الاجتماعي: https://www.aden-tm.net/news/270205

([13]) القاضي أنيس جمعان : التصنيف القانوني لجرائم الإبتزاز الإلكتروني / منصة اعرف حقك وقانونك: https://www.kurlye.com /

(1) التوعية بعدم نشر المعلومات الخاصة لهم ولعائلاتهم وأصدقائهم على وسائل التواصل، أو مشاركتها مع الغير وحتى المقربين، بمشاركة أسرارهم وصورهم والفيديوهات.

(2) عدم كشف كلمات المرور لأي حساب نهائيًا سواء كان حسابًا مصرفيًا أو بطاقة ائتمان، أو حسابًا على موقع بالإنترنت، ويجب تغيير كلمة السر باستمرار.

(3) التحري في قبول الصداقة والتحذير من الدخول على الروابط والإعلانات التي تتواجد بكثرة على المواقع الإلكترونية، أو المرسلة عبر وسائل التواصل الاجتماعي، والمراقبة والمتابعة والتفتيش لجميع المواقع التي يتصفحها أفراد العائلة، والملفات التي يحفظونها على أجهزتهم.

(4) عدم تصفح المواقع المجهولة، لاحتمال أن تكون مرتبطة بالبرامج التي تفتح الكاميرا الخاصة بك من أجل التقاط الصور، أو تكون مرتبطة ببعض الروابط المجهولة التي تسرق البيانات.

(5) عدم تصفح المواقع الجنسية على الجهاز الخاص بك؛ لأن كثيراً من هذه المواقع تسرق بيانات ومعلومات المستخدمين، وتجعلهم عرضة للابتزاز الإلكتروني.

(6) تثبيت برامج حماية من الفيروسات والاختراقات من أجل الحفاظ على سلامة الجهاز المستخدم.

وأخيراً كما أوضحت أنه نتيجة للتقدم العلمي والتكنولوجي المعاصر برزت الجريمة المعلوماتية التي أثرت بشكل كبير على مسائل الحقوق والحريات عبر العالم الرقمي، حيث مكنت تلك التكنولوجيا من انتهاك خصوصية الأفراد، والاطلاع على أسرارهم واستغلالها بشكل غير قانوني، وهذا ما تناولته في المطلب التمهيدي، الأمر الذي أدى إلى زيادة اهتمام المجتمع بالحق في حماية حرمة الحياة الخاصة على المستويين: الدولي والوطني، وهو ما سأتطرق إليه في المبحث الأول من هذه الدراسة.

المبحث الأول
الجهود الدولية في الحماية من الجريمة المعلوماتية

اهتم المجتمع الدولي اهتماماً كبيراً بمجال الوقاية من أخطر جرائم العصر الحديثة، وهي الجريمة المعلوماتية، وهذا ما أكدته الجماعة الدولية من خلال الدور الفاعل الذي تقوم به بإصدار المواثيق، وإبرام الاتفاقيات الدولية وعقد المؤتمرات الدولية، بغرض توفير أكبر قدر من الحماية من الجريمة المعلوماتية، ولتوضيح ذلك سأتناول في مطلبين دور منظمة الأمم المتحدة عموماً، ثم قرارات الجمعية العامة، ثم الحماية من الجريمة المعلوماتية في إطار المؤتمرات والاتفاقيات الدولية، وذلك على النحو الآتي:

المطلب الاول: دور منظمة الأمم المتحدة والجمعية العامة

سعت الأمم المتحدة منذ نشأتها إلى الاهتمام باحترام حقوق الانسان وحمايتها، ومنها جهودها في مجال حماية الجريمة المعلوماتية. وسنقوم في هذا المطلب ببيان أعمال

الأمم المتحدة إجمالاً، ثم نعرض بشكل خاص لقرارات الجمعية العامة للأمم المتحدة على النحو الآتي:

الفرع الأول: الدور العام لمنظمة الأمم المتحدة

تلعب منظمة الأمم المتحدة دور مهماً في الحفاظ على الأمن والسلم الدوليين، كما قامت بدور مهم في مجال مواجهة الجريمة المعلوماتية عبر إقرار العديد من الاتفاقيات، وعقد المؤتمرات الدولية، وبالإضافة إلى هذه الجهود الدولية، كانت الجهود الإقليمية التي تبنتها منظمات إقليمية بين بلدان يجمعها قاسم مشترك كالاتحاد الأوربي، وجامعة الدول العربية.

وفيما يتعلق بحق الإنسان في الحماية من الجريمة المعلوماتية، فقد رسخ حق الإنسان في الخصوصية في العديد من المواثيق الدولية والإقليمية، ابتداءً من الإعلان العالمي لحقوق الإنسان 1948م، حيث بدأت معه جهود الأمم المتحدة في مجال مواجهة الجريمة المعلوماتية، فكان أول عمل دولي يؤكد احترامه لحقوق الإنسان كافة، وهذا ما تضمنته المادة (12) الصريحة من الإعلان حيث نصت بأنه: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة، أو في شؤون أسرته، أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".

وتأكيداً لحماية حياة الفرد الخاصة وعبر حماية مباشرة وصريحة في القانون الدولي لحقوق الإنسان، جاء العهد الدولي للحقوق المدنية والسياسية 1966م، حين تم التأكيد على الحماية القانونية على هذا الحق، بموجب المادة (17) من العهد الدولي، التي نصت على أنه: "لا ينبغي أن يتعرض أحد لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه وسمعته"، وهذا النص ونص المادة (12) من الإعلان العالمي يؤكدان الحماية للحياة الخاصة من كل تدخل تعسفي، وحتما أن ذلك يشمل المجال التكنولوجي.

وتواصلت الجهود في حماية الحياة الخاصة من أخطار المعالجة الآلية للبيانات الشخصية في نظم الكمبيوتر وبنوك المعلومات، فظهرت هذه الجهود في مؤتمرات متخصصة بمسائل حقوق الإنسان والمتعلقة بالخصوصية، كما في مؤتمر استكهولم 1967م، ومؤتمر طهران 1968م- وسنشير له لاحقاً – وقد كان لهذه المؤتمرات أهمية بالغة في توجيه الاهتمام بمسائل حماية البيانات والخصوصية من المخاطر التقنية[14].

كما جاءت توصيات مؤتمر دول الشمال في ستوكهولم 1967م، لتؤكد ضرورة تقوية وسائل حماية الحياة الخاصة التقليدية التي لم تعد تتواءم مع التطور العلمي والتكنولوجي الحديث، وما بلغه من تهديدات واعتداءات جديدة لم تكن في الحسبان حال وضع التشريعات، مع حماية الفرد في حقه في الوحدة والعزلة

([14]) عقد مؤتمر ستوكهلم في الفترة من 22 إلى 23 من مايو 1967م تحت رعاية اللجنة الدولية للقانونيين، وقد شارك فيه مندوبون من دول عديدة هي النرويج و أمريكا وبريطانيا والهند واليابان والدانمرك وايسلندا والسويد والنرويج.

انظر: تقرير الامين العام للأمم المتحدة عن تأثير التطورات العلمية والتكنولوجية على حقوق الإنسان، ص 17 . مشار اليه لدى: د. فاروق محمد الأباصيري: عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت " ط 1" دار الجامعة الجديدة، 2002، ص 40.

من التطفل عليه باستخدام وسائل المراقبة والترصد والتجسس ([15]).

كما ورد إعلان دولي مُهمّ في هذا المجال، وهو الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لمصلحة السلم وخير البشرية، والذي صدر بموجب قرار الجمعية العامة للأمم المتحدة (3304 / د– 30) في 10 نوفمبر 1975م([16]).

ويُعدُّ مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين في ميلانو بإيطاليا عام 1985م، من أهم الأعمال الدولية، حيث انبثق عنه مجموعة من القواعد التوجيهية، وتم لاحقًا الانتقال بهذه القواعد إلى مؤتمر الأمم المتحدة الثامن في هافانا، لتتحول فيه إلى ما عرف بـ "مبادئ هافانا"، وتوجت بالمصادقة عليها في هافانا– كوبا – عام 1990م، وقد أكد المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح المجتمع، وذلك بهدف منع الجريمة على نحو قوي وفعال ([17]).

ويضاف إلى العمل الدولي قيام منظمة الأمم المتحدة بإنشاء المنظمة العالمية للملكية الفكرية التي ناقشت مسائل الخصوصية فيما يتعلق بحرية انتقال المعلومات، وتحديداً بالنسبة إلى اتفاقية التحرير للخدمات، وأقرت المنظمة بأن الخصوصية قيد عادل على عملية انتقال البيانات([18]).

وتواترت الجهود الدولية في الحماية من الجريمة المعلوماتية في تبني الأمم المتحدة عام 1989م، دليل يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية، وفي 1990/12/14م([19]).

وتوالى العمل الدولي في الحماية من الجريمة المعلوماتية، حيث عقد مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين في القاهرة عام 1995م، وكان من أهم توصياته العمل من أجل

- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية وتحسين أمن الحاسب الآلي والتدابير الفنية .
- اعتماد إجراءات تدريب كافية للموظفين والوكالات المسؤولة عن منع الجريمة والجرائم المتعلقة بالحاسب الآلي والتحري والإدعاء.

(د. محمود شريف بسيوني، الوثائق الدولية المعنية بحقوق الإنسان، المجلد الثاني، دار الشروق، القاهرة، 2003م)

([15]) د. أسامة عبد الله قايد، الحماية الجنائية وبنوك المعلومات، دار النهضة العربية، ط 3، 2008م، ص 13 .

([16]) اوضح هذا الاعلان: ضرورة التزام جميع الدول أن تتخذ تدابير فعالة، بما في ذلك التدابير التشريعية، لكفالة جميع المنجزات العلمية والتكنولوجية التي تستخدم لتأمين الاعمال الأكمل لحقوق الإنسان – ولا سيما حق الإنسان في الحياة الخاصة – والحريات الاساسية، دون تمييز بسبب العنصر أو الجنس أو المعتقدات الدينية

Marie – Christine pitti: Les libertés individuell à l'épreuve des nouvelles technologies de l'infromation, presses Universitaires de Lyon, 2007, p. 126.

([17]) مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين المعقود في ميلانو من 26 /أغسطس إلى 6 /سبتمبر 1985 واعتمدتها الجمعية العامة بقرارها 22/40 المؤرخ في 29 / نوفمبر 1985.

د. بولين انطونيوس ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، 2009م، ص 321، وهذه أهم مبادئ مؤتمر هافانا (1990م) للحد من جرائم التكنولوجيا المعاصرة:

([18]) تأسست المنظمة العالمية للملكية الفكرية "الويبو" (wipo) بموجب اتفاقية تم التوقيع عليها في استكهولم في 14 يوليو 1967م، ودخلت هذه الاتفاقية حيز التنفيذ سنة 1970, وتعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة ابتداء من 1974م.. (د. فؤاد بن صغير، التجارة الدولية، مطبعة فضالة المغرب، الطبعة الأولى، 2000 ص 52، الموقع الرسمي لمنظمة التجارة العالمية ع:– www.wto.org وانظر ايضا www.gatt.org

([19]) Francesco Miani: le cadre réglementaire des traitements de données personnelles effectues au sein de l'union européenne, revue trimestrielle de droit européen, Dalloz,n2, 2000, p283.

حماية حياة الإنسان الخاصة وملكيته الفكرية في مواجهة مخاطر التكنولوجيا، والعمل كذلك على التنسيق وتعزيز التعاون بين أعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها[20].

وتأكد اهتمام منظمة الأمم المتحدة بشأن مسألة مواجهة الجرائم المعلوماتية، بانعقاد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين الذي انعقد في فينا (10 – 17 ابريل 2000م)، وكذلك مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية الذي انعقد في بانكوك عام 2005م، وهدف إلى تعزيز منع الجريمة وتبادل الخبرات والمعرفة، ووضع السياسات والاستراتيجيات، وناقش منع الجريمة والعدالة الجنائية والتعاون الدولي [21]، كما عقدت منظمة الأمم المتحدة المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من (13/12) إبريل 2015م) بدولة قطر[22].

الفرع الثاني: قرارات الجمعية العامة للأمم المتحدة

قامت الجمعية العامة، وهي جهاز رئيس في الأمم المتحدة، بجهود كبيرة وفعالة في مجال مكافحة الجريمة المعلوماتية، من خلال إصدارها للعديد من القرارات المتعلقة بهذا الشأن. وتجدر الإشارة إلى أن قرارات الجمعية تحمل ثقلاً سياسيًا وأخلاقيًا قويًا لدى المجتمع الدولي، نذكر هنا بعضًا من تلك القرارات:

أولاً: قرار الجمعية العامة للأمم المتحدة رقم (2450)[23]: أصدرت الجمعية العامة في عام 1968م القرار رقم (2450) عن حقوق الإنسان والتقدم العلمي والتكنولوجي، عبرت فيه عن مشاركتها لمؤتمر طهران القلق من أن التقدم العلمي والتكنولوجي برغم ما منحه من آفاق واسعة أمام التقدم الاقتصادي والاجتماعي والثقافي، فإنه – مع ذلك – قد عرَض للخطر حقوق الأفراد والجماعات وحرياتهم؛ ولذلك فإن الأمر يتطلب اهتماماً متواصلاً ودراسات مستمرة، لحماية حقوق الإنسان وحرياته الأساسية، ومن أجل ذلك فقد دعت الجمعية العامة السكرتير العام بأن يقوم – مع الاستعانة بمن يستعين بهم، وبمعاونة اللجنة الاستشارية الخاصة بتطبيق العلوم والتكنولوجيا في التنمية، وبالتعاون مع الرؤساء التنفيذيين للوكالات المتخصصة – بدراسة المشكلات المتعلقة بحقوق الإنسان الناشئة عن التطورات العلمية والتكنولوجية، وبخاصة من النواحي الأربع التي اوصى بها المؤتمر سالفة الذكر.

ثانياً: قرار الجمعية العامة للأمم المتحدة رقم (2081) : وفي هذا القرار تبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول

---

(20) د. محمد الأمين ومحسن عبد الحميد أحمد معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية الرياض، ط 1، 1998، ص 19.

(21) عقد في بانكوك / تايلند. أيام 18–25 ابريل 2005م . (تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك، في الفترة 18–2005/4/25م، وثيقة رقم. A/CONF.203/14)

(22) وكان الموضع 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 الجمهور" وقررت الجمعية في قرارها رقم (6/184) انشاء حلقات عمل من بينها تعزيز منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة، منها الجرائم المعلوماتية. للمزيد أنظر : د. محمد أمين شوابكة، جرائم الحاسوب والانترنت / الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن، ط، 2009، ص 37.

(23) د. عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، القاهرة 2004م، ص 113 وما بعدها.

لحقوق الإنسان الخاص بأثر التقدم التكنولوجي على حقوق الأفراد المنعقد في طهران عام 1968م، الذي خرج بتوصيات تبرز خطر الحاسبات الإلكترونية على الخصوصية، وضرورة إيجاد آليات على المستوى الإقليمي أو الدولي لمحاربة أجهزة التجسس([24]).

ثالثاً: قرار الجمعية العامة (56/121) : صدر بتاريخ (19/ 12/ 2001م) بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات"، يدعو هذا القرار الدول الأعضاء إلى وضع تشريعات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات.

رابعاً: قرار الجمعية العامة (57/239) : صدر بتاريخ (2003/1/30م) بشأن إنشاء ثقافة عالمية للأمن السيبراني ودعوة الدول الأعضاء إلى التعاون وتعليم ثقافة الأمن السيبراني.

خامساً: قرار الجمعية العامة رقم (167 / 68) : جاء بتاريخ 18 ديسمبر 2013م تحت عنوان "الحق في الخصوصية في العصر الرقمي"، والذي يعتبر مرحلة متطورة للجهود الدولية التي تهدف إلى حماية الحق في الخصوصية المعلوماتية، حين عبرت الجمعية عن قلقها بشأن القدرة المتنامية للمؤسسات الحكومية على الوصول إلى خصوصية الأفراد من خلال المراقبة عبر الوسائل التكنولوجية سواء كان الأشخاص المراقبون داخل الدولة أو خارجها، وقد تضمن هذا القرار ست توصيات تهدف إلى الحد من الأثر السلبي الذي يمكن أن تخلفه مراقبة الاتصالات، واعتراضها وجمع البيانات على حقوق الإنسان، وأكدت أن الحق في الخصوصية هو حق من حقوق الإنسان، ومشددة على أن حقوق الإنسان المحمية خارج الفضاء الإلكتروني يجب أن تكون محمية داخل الفضاء الإلكتروني، كما يجب على الدول الأعضاء أن تعيد النظر في إجراءاتها وممارستها وتشريعاتها المتعلقة بالمراقبة الإلكترونية، وذلك بهدف تأكيد الحق في الخصوصية، تنفيذاً لالتزاماتها بموجب القانون الدولي لحقوق الإنسان([25]).

سادساً: قرار الجمعية العامة رقم (243 / 79) : الصادر بتاريخ 2024/12/24م، ويمثل خطوة تاريخية بإقرار الجمعية العامة لاتفاقية مكافحة الجرائم المعلوماتية (السيبرانية)، وهو ما يمثل أبلغ حماية حديثة لخصوصية الإنسان وضحايا الاستغلال المعلوماتي بكافة أشكاله، كما نصت الاتفاقية على

([24]) أوصى القرار رقم (11) منه باحترام خصوصية الإنسان على ضوء الانجازات المحققة في تقنيات التسجيل، وحماية الشخصية الإنسانية، واستخدام الإلكترونيات التي قد تؤثر على حقوق الشخص، والقيود التي يجب وضعها على هذا الاستخدام، مع لزوم التوازن بين التقدم العلمي والتكنولوجي وبين رقي الإنسانية الفكري والثقافي والاخلاقي. أنظر : http://hrlibrary.umn.edu/arab/b006.html

وجاء في مؤتمر طهران .. إن المؤتمر الدولي لحقوق الإنسان ... يعلن علي الملأ رسميا (وفقا للبنود 16، 18) ما يلي :

- ان الحق في الخصوصية يضمن حق الفرد في الا تنشر معلومات تتعلق بحياته الخاصة أو بشخصيته لم يكن ليكشف عنها هو نفسه.
- ان تقدم العلوم والتكنولوجيا قد جعل بالامكان انتهاك رمة الحياة الخاصة للافراد أو المساس بكرامتهم وبحرمة شخصيتهم عن طريق وسائل التلصص على المخابرات الهاتفية وادوات استراق السمع الإلكترونية والات التصوير والتسجيلات الخفية والمستحدثات الصيدلانية.

(د. يونس عرب، جرائم الحاسوب، دراسة مقارنة، رسالة ماجستير، الجامعة الاردنية، 1994م، ص 125، وراجع: الوثيقة النهائية لمؤتمر طهران، ص 148).

([25]) موقع الأمم المتحدة : https://www.un.org/ar/ga/68/resolutions.shtml

تفعيل التعاون القضائي وتبادل الأدلة الاليكترونية بين الدول، وستدخل المعاهدة الجديدة حيز التنفيذ بمجرد أن تصادق عليها (40) دولة عضوا أمام الجمعية العامة، وهي التي سبق وأن وقعت عليها رغم معارضة أمريكا للاتفاقية ([26])، وتعد أول معاهدة دولية لمكافحة الجريمة المعلوماتية يتم التفاوض عليها بين الدول الأعضاء في المنظمة العالمية منذ أكثر من عشرين عاماً. وتهدف الاتفاقية إلى منع ومكافحة الجرائم المعلوماتية بكفاءة وفعالية أكبر، بما في ذلك من خلال تعزيز التعاون الدولي وتقديم المساعدة الفنية ودعم بناء القدرات، وخاصة للدول النامية، وتقر الاتفاقية وهي الملزمة قانوناً بالمخاطر الكبيرة الناجمة عن إساءة استخدام تكنولوجيا المعلومات والاتصالات وبالتالي القيام بأنشطة إجرامية على نطاق ووتيرة غير مسبوقين([27]).

وبالإضافة إلى جهود الأمم المتحدة، فقد عملت سائر المنظمات الدولية بجهد على تنظيم وحماية المعلومات الخاصة وتنظيم تدفق المعلومات وانتقالها، ومن هذه المنظمات منظمة التعاون الاقتصادي والتنمية، والتي بدأت منذ عام 1978م بوضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات([28])، أيضاً المنظمة العالمية للملكية الفكرية ومنظمة التجارة العالمية التي ناقشت مسائل الخصوصية فيما يتعلق بحرية انتقال المعلومات، وتحديداً بالنسبة إلى اتفاقية التحرير للخدمات، وأقرت المنظمة بأن الخصوصية قيد عادل على عملية انتقال البيانات.

ومن خلال ما سبق يتضح أن الأمم المتحدة والجمعية العامة بشكل خاص، قد قامتا بجهود كبيرة في سبيل توفير الحماية من الجريمة المعلوماتية من خلال تبنيهما لإصدار المواثيق والاتفاقيات والقرارات التي توفر الحماية للمجتمعات من هذه الجرائم.

المطلب الثاني
الحماية من الجريمة المعلوماتية في اطار الاتفاقيات والمؤتمرات الدولية وقوانين الأونسيترال النموذجية

اهتمت العديد من الاتفاقيات الدولية والمؤتمرات العالمية والمحلية بحرمة الحياة الخاصة في إطار المعلوماتية، وإظهار وجه الخطورة للتقنية الحديثة، وبيان مخاطرها على حقوق الإنسان وحرياته الأساسية، وفيما يلي نعرض الحماية في إطار الاتفاقيات الدولية الخاصة بجرائم المعلوماتية، ثم المؤتمرات العالمية والإقليمية المعنية بالحريمة

([26]) موقع الأمم المتحدة : https://news.un.org/ar/story/2024/08/1133441
ولأن المصدر هنا هو موقع الأمم المتحدة، فان الحاصل أن الأغلبية العادية البسيطة هي المطلوبة، أي أن الدول الاربعين كانت أكثر من نصف الحاضرين المصوتين في الجمعية العامة اثناء مناقشة مشروع الاتفاقية، وذلك وفقاً للمادة (18) من ميثاق الأمم المتحدة، والمادة (85، 86) من النظام الداخلي للجمعية العامة، وهذا بخلاف المادتين (83، 84) التي يتطلب التصويت فيها أغلبية ثلثي أصوات الحاضرين المصوتين.

([27]) ركّزت الاتفاقية على ثلاثة أهداف رئيسية، وهي: تحسين طُرق منع الجرائم الإلكترونية ومواجهتها، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية، وتوفير المساعدة الفنية وبناء القدرات لا سيّما للبلدان النامية. وفي سلسلة المقالات هذه، سننظر في القدرة الفعلية للاتفاقية على تحقيق الأهداف التي حددتها.

([28]) منظمة التعاون الاقتصادي والتنمية Organization for Economic Co-operation and Development – OECD :
هي منظمة دولية تأسست عام 1961م، ومقرها باريس وتضم في عضويتها 38 دولة متقدمة اقتصادياً، وغرضها الرئيس تحقيق اعلى مستويات النمو الاقتصادي لأعضائها وتناغم التطور الاقتصادي مع التنمية الاجتماعية انظر حول هذه المنظمة وانشطتها موقعها الشامل على الانترنت: www.oecd.org

المعلوماتية، ثم نعرض القوانين الأونسيترال النموذجية، وذلك في الثلاثة الفروع التالية:

الفرع الأول: الاتفاقيات الخاصة بجرائم المعلوماتية

تقوم الاتفاقيات الدولية بدور مهم في التنسيق بين التشريعات المختلفة للدول، وهي من أبرز صور التعاون الدولي في مجال حماية حق الخصوصية في المجال الرقمي من الاعتداءات الإليكترونية.

وتعد التجربة الأوروبية الاكثر نجاحاً ونضجاً على مستوى العالم في حماية الخصوصية، لا سيما في مجال المعلوماتية، وقد كان لمجلس أوروبا دور كبير في عقد الاتفاقية الأوربية لحقوق الإنسان والحريات العامة لعام 1950م، والتي أوجبت المادة (8) من هذه الاتفاقية حماية الأفراد من التدخل والاعتداء على حياتهم الخاصة وحياة أسرهم، كما قررت المادة (10) من هذه الاتفاقية وجوب حماية حق الوصول ونقل المعلومات[29]، كما كان للاتحاد الأوربي دور مؤثر في حماية الحق في الخصوصية؛ إذْ صدر عن الاتحاد عدة تعليمات بهذا الشأن[30].

وفيما يلي أهم الاتفاقيات الدولية المعنية بالحماية ومكافحة جرائم المعلوماتية كالتالي:

أولاً : الاتفاقية الأوروبية لحماية الافراد من مخاطر المعالجة الآلية للبيانات الشخصية 1981م

تعد الاتفاقية الأوروبية لحماية الأفراد من مخاطر التعدي على البيانات الشخصية رقم 108 في 28 يناير 1981م، هي أول تشريع أو صك دولي يهتم بحماية البيانات؛ حيث جاءت الاتفاقية في ظل الانفتاح الواسع للإنترنت الذي أتاح التبادل الواسع لمختلف أنماط المعلومات وخلق بيئة للاستثمار والأعمال فيما يعرف بالأسواق الافتراضية أو بيئة الأعمال الإلكترونية، وقد كفلت الاتفاقية ضمان حقوق الفرد بغض النظر عن الجنسية أو الإقامة واحترامها في مواجهة الاستخدام الآلي للمعلومات ذات الطابع الشخصي، كما تضمنت الاتفاقية عدة مبادئ تمثلت في الحد الأدنى من الاحتياطات التي يجب أن تتضمنها التشريعات الداخلية للدول أطراف المعاهدة لحماية الأفراد من إساءة استخدام البيانات المعالجة إلكترونيًّا، وضرورة الحصول على البيانات الشخصية من مصادر مشروعة، وأن تكون البيانات صحيحة

(29) ومن الاعمال الاوروبية المتتالية صدور الدليل الأوروبي لعام 1995م بشان حماية الأفراد من مخاطر المعالجة الالية للبيانات الشخصية وحرية انتقالها، والدليل الأوروبي لعام 1997م بشان معالجة البيانات الشخصية، وحماية الحياة الخاصة في قطاع الاتصالات السلكية واللاسلكية، والدليل الأوروبي لعام 2002م بشان معالجة البيانات الشخصية، وحماية الحياة الخاصة في قطاع الاتصالات الاليكترونية، والدليل الأوروبي لعام 2006م بشان الاحتفاظ او الابقاء على البيانات التي تستخلص التي تعالج، في إطار توفير خدمات الاتصالات الاليكترونية او الشبكات الاليكترونية المتاحة للجمهور. (د. محمد أمين المداني، النظام الأوروبي لحماية حقوق الإنسان، مطبوعات مركز التوثيق والاعلام، وزارة حقوق الإنسان المغربية، يناير 2004م، ص 105).

(30) منها التعليمات المتعلقة بحماية الأفراد من أنشطة خزن ونقل البيانات والتعليمات المتعلقة بحماية الأفراد من أثر التطور التقني لمعالجة البيانات، والتوجيه الأوربي رقم (85) الصادر من البرلمان الأوربي لسنة 2002م والمتعلق بالمعالجة الآلية للبيانات وحماية الخصوصية

MATTATIA Fabrique, Traitement des donnes personnelles– Le guide juridique– la loi informatique et libertés de la CNIL jurisprudences, Edition Eyrolles, Paris, 2013, p.13.

ومتفقة مع الغرض الذي وضعت من أجله، وأن تكون المعلومات حديثة، كما أكدت على اتخاذ التدابير التشريعية والتنظيمية لضمان ملاحقة مرتكبي هذه الجرائم وكشفها وتوفير قواعد ملائمة للتحري والتحقيق والضبط والتفتيش والمحاكمة، مع التركيز على أهمية التعاون المحلي والإقليمي والدولي مع وجوب إقامة التوازن بين متطلبات تنفيذ القانون وبين وجوب احترام الحقوق الأساسية والسيادة، ولأن الاتفاقية جاءت حصيلة جهود دولية وإقليمية فقد أكدت الاتفاقية على أهمية ما أنجز من جهود في حقل جرائم الكمبيوتر من قبل الأمم المتحدة ومنظمة التعاون الاقتصادي والتنمية والاتحاد الأوربي ومجموعة الدولة الصناعية (مجموعة الثمانية)([31]).

ثانياً : اتفاقية بودابست لسنة 2001م المتعلقة بالإجرام المعلوماتي([32])

أكدت الاتفاقية على حماية الحياة الخاصة في مجال المعلوماتية، من خلال النص على تجريم الأفعال التي تشكل مساسًا بسرية البيانات والنظم المعلوماتية (المواد 2– 6 من الاتفاقية) مثل الوصول غير المشروع للنظام المعلوماتي، والتعدي على البيانات الشخصية عن طريق اتلافها أو محوها أو تغييرها بدون وجه حق، والتعدي على سلامة النظام المعلوماتي، كما جاء في نص المادة الثالثة على جريمة الاعتراض غير القانوني باستخدام الوسائل الفنية للبيانات المتداولة إلكترونيًّا في الحواسيب عبر شبكة الانترنت، واختصت المادة الرابعة بالنص على ضرورة توحيد أطراف الاتفاقية للجهود بغية تبني الإجراءات التشريعية التي تجرم الاعتداء على سلامة البيانات من أجل ضمان سلامة المنظومة البيانية للاتصالات الإلكترونية، بالإضافة إلى النص على جرائم التزوير والغش المعلوماتي، وذلك عن طريق إدخال بيانات وهمية أو تغييرها أو حذفها (المواد 7، 8 من الاتفاقية)، كما تضمنت الاتفاقية مختلف القواعد الإجرائية المتعلقة بالبحث والتحري عن الجريمة المعلوماتية، وتتكون الاتفاقية من (48) مادة، تميزت بكون (22) مادة تنظم القواعد الإجرائية، والتي تهدف أساسا إلى وضع سياسية جنائية مشتركة بين الدول من أجل حماية الأفراد من الجرائم المعلوماتية المتطورة.

وتعتبر اتفاقية بودابست أول معاهدة دولية شاملة بشأن الجريمة الإلكترونية، وقد شكلت إطاراً مرجعيًّا للعديد من الدول في تطوير تشريعاتها

([31]) Daniel Kaplan, Informatique, libertées, identities, Fyp Edition,1er avril.2010,P10.

وضعت الاتفاقية الخاصة بحماية الأفراد للتوقيع في يناير 1981م، وبدأ السريان الفعلي لهذه الاتفاقية في أكتوبر 1985م، وقد وقعت على هذه الاتفاقية كل من النمسا، بلجيكا، الدنمارك ألمانيا الغربية، فرنسا، اليونان، أسلندا، إيطاليا، لوكسمبورغ، النرويج البرتغال، السويد، تركيا –المملكة المتحدة، وقد صدقت عليها كل من فرنسا وألمانيا والنرويج واسبانيا والسويد. منظمة التعاون والتنمية في الميدان الاقتصادي، المبادئ التوجيهية التي تحكم حماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية:
https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

([32]) تعد أول اتفاقية ذات طابع دولي يتبناها المجلس الأوروبي في هذا المجال، حيث ضمت كل الدول الأوروبية وغير الأوروبية، حيث تم السماح بالانضمام لدول من خارج دول الاتحاد الأوروبي مثل جنوب إفريقيا والمغرب وتونس واليابان والولايات المتحدة الأمريكية، وقد دخلت حيز التنفيذ في سنة 2002م. (د. هلالي عبد اللاه احمد –: الجوانب الموضوعية والاجرائية لجرائم لمعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م، دار النهضة العربية، القاهرة، 2006م، ص 67 وما بعدها، د. محمد امين الشوابكة،، جرائم الحاسوب والانترنت / الجريمة المعلوماتية، مرجع سابق، ص 72).

الوطنية، وساهمت الاتفاقية في تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، ممّا سهل التحقيقات والملاحقات القضائية عبر الحدود، وساعدت الاتفاقية في توحيد القوانين الوطنية للدول الأعضاء، مما جعل مكافحة الجريمة الإلكترونية أكثر فعالية، ووفرت الاتفاقية إطاراً قانونيًّا للتعامل مع التحديات الجديدة التي تطرحها التكنولوجيا الحديثة في مجال الجريمة.

الجدير بالذكر أنه إلى جانب الاتفاقيات الخاصة في أوروبا التي جرمت كل اعتداء يمثل جريمة معلوماتية، فإن هناك آليات ووسائل قوية أخرى لحماية الأفراد من هذه الجريمة (تأتي ضمن آليات حماية حقوق الإنسان عموماً هناك)، حيث بإمكان أي فرد داخل أوروبا إذا ما حصل وانتهكت أي من حقوقه بهذا الصدد، أن يلجأ بتقديم شكوى إلى اللجنة الأوروبية، أو إلى المحكمة الاوروبية، أو إلى لجنة الوزراء، إضافة لنظام التقارير الملزمة للدول، وحق الشكوى مضمون وفق ميثاق الحقوق الأساسية للاتحاد الأوروبي 2000م، وكلها ضمانات وآليات متقدمة في الحماية (وتناولها لا يتسع له المجال هنا في بحثنا).

ثالثاً : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010م:

تبنت جامعة الدول العربية أول اتفاقية عربية لمكافحة جرائم تقنية المعلومات في 21 يناير 2010م، وجاءت الاتفاقية في إطار تعزيز التعاون والدعم بين الدول العربية في مجال تقنية المعلومات([33])، بحيث سارت الاتفاقية على نهج الاتفاقية العالمية بودابست من خلال إقرارها في الفصل الأول الهدف من الاتفاقية المتمثل في تعزيز التعاون والدعم بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم وحفاظاً على أمن الدول العربية في هذا المجال.

وقد ألزمت الاتفاقية الأطراف بتجريم شتى أساليب الاعتداء على حقوق الأفراد في المجال الإلكتروني، المنصوص عليها بالفصل الثاني منها، والمعنون(بالتجريم) ، والذي ركزت فيه على تجريم الدخول غير المشروع، وكذا الاعتراض غير القانوني للبيانات الشخصية، وفي المادة (14) نصت بشكل مباشر على تجريم الاعتداء على حرمة الخصوصية بواسطة تقنية المعلومات([34]).

ومن خلال ما سبق التطرق إليه يتضح أن الاتفاقيات الأوروبية شهدت تطوراً كبيراً في مجال الحماية من الجريمة المعلوماتية، مقارنة بالاتفاقيات العربية القليلة والتي لم تواكب العمل القانوني الإنساني العالمي والإقليمي.

([33]) د. محمد نور فرحات، في كتاب المعايير الدولية وضمانات حماية حقوق الإنسان في الدستور والتشريعات المصرية، المواثيق الإقليمية لحقوق الإنسان، ملاحظات اولية، برنامج الأمم المتحدة الانمائي، القاهرة 2006م، ص 51، السيد ابو الخير، نصوص المواثيق الدولية والاعلانات والاتفاقيات لحقوق الإنسان، ايتراك للنشر والتوزيع، القاهرة، 2005م، ص25.

([34]) أشارت الاتفاقية لأنواع الجرائم التي تقع عن طريق الكمبيوتر والانترنت بصفة عامة، وأحالت إلى التشريعات الداخلية كلما يتعلق الأمر بأركان هذه الجرائم وكذلك العقوبات التي تطبق عليها. (محمود أحمد عبابنة، مرجع سابق، ص 170 وما بعدها).

ويرى الباحث أن أفضل وأنسب أنواع التعاون هو التعاون الثنائي فيما بين الدول لمكافحة الجريمة المعلوماتية، حيث يتم التفاهم وحل مسائل الاختصاص سريعاً، وبعيداً عن الخلاف في التجمعات الدولية.

الفرع الثاني: المؤتمرات الدولية الخاصة بالحماية من جرائم المعلوماتية

تأكيداً على أن موضوع الحق في الحياة الخاصة من أولويات الأسرة الدولية، فقد عقدت مؤتمرات دولية بشأن هذا الحق، خاصة بعد الانتهاكات التي أصبح الفرد، وكل المجتمع، يتعرض لها بصفة متزايدة وخطيرة، بسبب ما بلغته التطورات العلمية والتكنولوجية، ومن أهم هذه المؤتمرات:

أولا: مؤتمر الامم المتحدة في نيوزيلندا 1961م :

نوقشت في هذا المؤتمر مشكلة التقدم العلمي في مجال التحقيق الجنائي، ومدى خطورة ذلك على الحق في الحياة الخاصة، مثل المراقبة الهاتفية والتسجيل الإلكتروني للأحاديث الخاصة، الأمر الذي يشكل انتهاكا صريحا لحق الشخص في حياته الخاصة؛ حيث أكد المجتمعون في هذا المؤتمر على ضرورة أن تقوم الدولة بوضع قيود وضوابط معينة على مراقبة المحادثات الهاتفية وتسجيلها، والمقصود بها هنا ما يكون من إجراءات تقوم بها الأجهزة الخاصة بالدولة([35])، وترتب على ذلك جملة من الضمانات منها ألّا يكون إجراء التسجيل والمراقبة إلا عندما يكون الأمر مهمًّا وضروريًّا، للكشف عن هذه الجريمة، وأيضاً ضرورة علم الشخص بالحد الأقصى المسموح به، والجائز قانوناً للتصنت، أو المراقبة وتسجيل الأحاديث الخاصة.

ثانياً : مؤتمر مونتريال عام 1968م ومونتريال 2007م :

أوصى مؤتمر مونتريال عام 1968م بالعناية بالأخطار الجديدة بسبب التطورات العلمية الحديثة، مثل وسائل التطفل الإليكتروني والوسائل السمعية والبصرية وأثرها على خصوصيات الأفراد([36]).

ثالثاً : المؤتمر الدولي السابع للمركز الدولي للدراسات والبحوث (مدريد/ 1984م) :

نظم المركز الدولي للدراسات والبحوث الاجتماعية والجنائية والإسلامية المؤتمر السابع له الذي عقد في مدريد عام 1984م ([37])، وقد اهتم المؤتمر بموضوع حقوق الإنسان والحريات العامة وعمل الشرطة، ومما صدر عنه من توصيات بشأن حماية الحق في الحياة

([35]) د. اسامة عبد الله قايد، مرجع سابق، ص 81.

([36]) تمت الدعوة في هذا المؤتمر إلى تشجيع المنظمات والهيئات غير الحكومية للقيام بدورها في مواجهة الاثار السلبية المترتبة للعلم الحديث والتقدم التكنولوجي في مجال الإثبات الجنائي التي تشكل انتهاكا صريحا لحق الشخص في الحياة الخاصة، مثل أجهزة التصوير التي لا تراها العين المجردة، وكذلك اجهزة التسجيل، وان تقوم هذه المنظمات برفض الاعتراف بالأدلة المتحصل عليها من استخدام هذه الأساليب.
(د. فادية ابو شهبة، الحق في الخصوصية، المجلة الجنائية القومية، مجلد 4 (مارس، يوليو، نوفمبر)– 1997م، ص 302).

كما انعقد المؤتمر الدولي التاسع والعشرين لمفوضي الخصوصية وحماية البيانات في مدينة مونتريال بكندا في الفترة من 25 / 28 سبتمبر 2007م.، وتناول مدى مشروعية قيام حكومات الدول بأخذ البيانات الشخصية المعالجة آلياً والخاصة بالمسافرين عبر وسائل النقل وحفظها، وذلك لأغراض مكافحة الارهاب والمحافظة على الامن القومي.
http://www.unep.fr/ozonaction/information/mmcfiles/7473-a-OASI2010_OutOfTheMaze.pdf

([37]) د. فادية ابو شهبة، المرجع السابق، ص 303.

الخاصة أنه "يجب أن يكون استخدام الأساليب الحديثة في مراقبة الأفراد بالوسائل السمعية والبصرية بالقدر الضروري وبالطرق المشروعة، لكل ما يترتب عليها من انتهاك لحرمة الحياة الخاصة"[38].

رابعاً: المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر 1994م :

عقد المؤتمر في (4 / 9 أكتوبر 1994م) البرازيل / **ريودي جانيرو**، وأوصى المؤتمر بأن تتضمن الحد الأدنى للأفعال المتعين تجريمها، واعتبارها من قبيل جرائم الكمبيوتر ما يلي[39]:

1. الاحتيال أو الغش المرتبط بالكمبيوتر، ويشمل الادخال، والإتلاف، والمحو لمعطيات الكمبيوتر أو برامجه، أو القيام بأية أفعال تؤثر بمجرى المعالجة الآلية للبيانات، وتؤدي إلى إلحاق الخسارة، أو فقدان الحيازة، أو ضياع ملكية شخص، وذلك بقصد جني الفاعل منافع اقتصادية له أو للغير.
2. التزوير عبر الكمبيوتر أو التزوير المعلوماتي، ويشمل إدخال أو إتلاف أو محو المعطيات أو البرامج، أو أية أفعال تؤثر على المجرى الطبيعي لمعالجة البيانات ترتكب باستخدام الكمبيوتر.
3. الإضرار بالبيانات والبرامج "الاتلاف"، وتشمل المحو والاتلاف والتعطيل والتخريب لمعطيات الكمبيوتر وبرامجه.
4. تخريب وإتلاف الكمبيوتر، وتشمل الإدخال أو المحو أو الإتلاف أو التخريب، أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر، أو نظام الاتصالات "الشبكات".
5. الدخول غير المصرح به: وهو التوصل أو الولوج دون تصريح إلى نظام، أو مجموعة نظم عن طريق انتهاك إجراءات الأمن.
6. الاعتراض غير المصرح به، وهو الاعتراض عن طريق وسائل فنية للاتصال توجه لنظام كمبيوتر أو عدة نظم أو شبكة اتصالات.

خامساً: المؤتمر الدولي لأمن المعلومات الإلكترونية (مسقط / 2005م):

انعقد هذا المؤتمر في العاصمة العمانية مسقط في الفترة من 18 إلى 20 ديسمبر 2005م، وكان الهدف من وراء انعقاده توعية المؤسسات والأفراد بمخاطر الإنترنت، وتوعيتهم بالقوانين الموجودة في الوقت الحالي، ومدى كفايتها في توفير الحماية اللازمة للحق في الحياة الخاصة وأمن المعلومات، في ظل التنامي الكبير وانتشار المواقع الإلكترونية على الشبكة العنكبوتية[40].

([38]) مجلة الامن العام، القاهرة، يناير 1985م، عدد 108، ص 91.

([39]) د. هلالي عبد اللاه احمد، تفتيش نظم الحاسب الالي وضمانات المتهم المعلوماتي، النسر الذهبي، القاهرة، 2000م، ص 5.

([40]) د. ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009، ص 90، http://www.albayan.ae/economy/1135159674001-2005-12-22-1.128467

ومن توصيات المشاركين في المؤتمر: التأكيد على ضرورة تبني سياسة مشتركة تحقق أمنا معلوماتيًّا للقضاء على الآثار السلبية التي تهدد البيانات الشخصية بالفناء، والعمل على وضع تشريع متكامل لحماية البيانات والخصوصية على الأنترنت، لا سيما في ظل الانتشار والاستخدام اللامتناهي للشبكة العنكبوتية في شتى المجالات.

سادساً: المؤتمر الدولي الأول لمكافحة جرائم تقنية المعلومات (الشارقة/ 2006م) :

يعتبر هذا المؤتمر شاملاً من حيث دراسة وبحث إشكالية الجرائم المعلوماتية من حيث المفهوم والمكافحة على المستوى الوقائي والعلاجي، وفتح النقاش لدراسة التوجهات المستحدثة في هذا المجال والسعي لتبادل الخبرات في مجال مكافحة جرائم تقنية المعلومات([41]).

سابعاً: المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الأنترنت 2008م ([42]):

تناول مناقشة العديد من الموضوعات المرتبطة بالاستخدام غير المشروع لتقنية المعلومات والانترنت، مثل حماية البيانات المتداولة عبر الأنترنت، والتجارة الإلكترونية والحكومة الإلكترونية([43]).

وانتهى المؤتمر إلى التوصية بالإسراع بالانضمام إلى اتفاقية مكافحة الجرائم المعلوماتية "بودابست" وتبادل الخبرات والتجارب الدولية بين الدول بعضها ببعض لعرض النظم القانونية والتقنية لأمن المعلومات والإسراع في إصدار تشريعات حول الخصوصية، وأمن المعلومات، والعقوبات الرادعة لارتكاب مثل هذه الأفعال غير المشروعة.

ثامناً: المؤتمر الدولي الثاني والثلاثون لمفوضي الخصوصية وحماية البيانات– القدس 2010م([44]):

عقد هذا المؤتمر في مدينة القدس بفلسطين المحتلة في الفترة من 27 / 29 أكتوبر 2010م بشأن "حماية الحياة الخاصة في خدمات الشبكات الاجتماعية"، وقد أوصى المؤتمر بوجوب الانضمام إلى الاتفاقية الأوروبية – المفتوحة – لحماية الأفراد من مخاطر المعالجة الآلية للبيانات – بودابيست 2001م – والبروتوكول الإضافي الملحق بها، إضافة إلى تشجيع المنظمات الدولية والمحلية وعناصر المجتمع المدني المهتمة بالحياة الخاصة وحماية البيانات لدعم الدعوة إلى مؤتمر حكومي دولي لمناقشة مخاطر التقدم العلمي على حرمة الحياة الخاصة والبيانات الشخصية.

وللإشارة والبيان فإنه –ومع الأهمية لهذا المؤتمر– فلا بد أن نكشف هنا عمّن يريد أن يجمل نفسه دوليًّا

([41]) عقد هذا المؤتمر بالشارقة / الإمارات العربية المتحدة في 11/8/ 2006م (محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإليكترونية، مكتبة الوفاء ط 1، الاسكندرية، 2014، ص 204).

([42]) http://news.wata.cc/news.php?action=vfc&id=748

([43]) انعقد المؤتمر في القاهرة في الفترة من (2 / 4 يونيو 2008م).

([44])

http://www.justice.gov.il/PrivacyGenerations/Ar/privacy.htm

كما انعقد مؤتمر في مكسيكو من 2 / 3 نوفمبر 2011م، تحت عنوان حماية الحياة الخاصة في عصر العولمة، ومن لموضوعات التي تناوله هذا المؤتمر هي كيفية حماية البيانات الشخصية في زمن الكوارث الطبيعية أو غير الطبيعية، واوصى هذا المؤتمر على ضرورة العمل على توفير ضمانات مناسبة لحماية البيانات الشخصية في زمن الكوارث، وتعويض اصحاب البيانات الشخصية عن الاضرار التي قد تلحق بهم نتيجة للمساس بسريتها.

http://www.unep.fr/ozonaction/information/mmcfiles/7473-a-OASI2010_OutOfTheMaze.pdf

من خلال احتضانه لمؤتمرات إنسانية، وهو في حقيقته المثل الصارخ بعينه في انتهاك حق الخصوصية للأفراد وحقوق الإنسان عموماً.

فإسرائيل تنتهك كل عناصر الحياة للإنسان والحياة الخاصة للفلسطينيين، وتقوم بالتجسس على الأفراد ليلاً ونهاراً، حيث لا حرمة لديهم لمسكن أو لحق الفرد في اتصالاته أو صحته، وكل الجرائم لحقوق الإنسان قائمة في كل فلسطين المحتلة، ولا زالت الانتهاكات دون توقف أو منعة من شرعية دولية، أو حتى لقوانينها الداخلية التي تنتصر – بكل عنصرية – للمواطن اليهودي.

ولعل إرهابها الاليكتروني – الحربي – الذي شهدته غزة ولا زالت تعيشه، وأمام مسمع ومرأى العالم، خلال عامين تقريباً، ضمن عدوانها الكبير، ولا زال سلوكها هذا يمثل أسوأ وأعنف إجرام العصر بكل صوره وأشكاله.

الفرع الثالث
لحماية المعلوماتية في إطار قوانين الأونسيترال النموذجية

تعد قوانين الأونسيترال النموذجية هي العنصر المتناول في مجال الحماية من الجريمة المعلوماتية، وفيما يلي نعرض القوانين النموذجية على النحو الآتي:

أولاً : قانون الأونسيترال النموذجي:

اقتناعًا من الدول بضرورة منع هذه الجرائم ومكافحتها خاصة، وأن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، تم صياغة قانوني الأونسيترال النموذجي بشأن التجارة الإلكترونية، والآخر بشأن التوقيعات الإلكترونية[45] كما يلي:

1 - قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية 1996م

يُعَدُّ هذا القانون من أهم الجهود الدولية في مجال مكافحة الجرائم المتعلقة بالمعلوماتية على المستوى الدولي، وقد كان لبنة للعمل الكبير الذي قامت به "الأونسيترال" في سبيل وضع نصوص نموذجية لتزويد المشرعين الوطنيين بمجموعة قواعد مقبولة دوليًا ترمي إلى تذليل العقبات القانونية وتعزيز القدرة على التنبّؤ بالتطورات القانونية في مجال التجارة الإلكترونية لمواجهة جرائم المعلوماتية في مجال التجارة الإلكترونية، وقد لقي هذا القانون قبولا من طرف مشرعي الدول والمتعاملين، لا سيما بعد أن اعتمدته لجنة الأمم المتحدة سنة 1996م[46].

([45]) د. شمس عبدالله العمرو " قانون الأونسيترال النموذجي": hnews.net/article/227724

([46]) وتنطبق نصوص هذا القانون على أي نوع من المعلومات التي تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية، بحيث يتم استلامها أو تخزينها بوسائل إلكترونية، ويتم تبادل هذه البيانات من خلال نقلها إلكترونيا من حاسوب إلى آخر باستخدام معيار متفق عليه، مع الأخذ بعين الاعتبار تفسير هذا القانون لمصدره الدولي لضرورة توحيد تطبيقه. (قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996 : https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook.pdf

2 - قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية 2001م:

يُعدُّ هذا القانون تكملة للجهود التي بذلتها لجنة "الأونسيترال" في سبيل مكافحة الجرائم المعلوماتية المتعلقة بالتجارة الدولية، حيث تكفّل بوضع قواعد موحدة من شأنها حماية التوقيع الإلكتروني، وهو ما كرسته الكثير من الدول في تشريعاتها الداخلية، وينطبق هذا القانون حيثما تستخدم توقيعات إلكترونية، خاصة بعدما أصبح التوقيع بمفهومه التقليدي لا يستجيب لمتطلبات السرعة والحداثة التكنولوجية، حيث إنه أمام هذه التطورات، تلاشت وظيفة التوقيع التقليدي ليحل محله التوقيع الإلكتروني، وهو عبارة عن كود سري أو شفرة سرية يتم الحصول عليه بعد اتباع جملة من الإجراءات[47].

ثانياً : القانون العربي النموذجي الاسترشادي 2003م ([48]):

تضمن القانون بشأن مكافحة جرائم إساءة استخدام تقنية المعلومات، منع نسخ برامج الكمبيوتر بدون إذن، وكل من يقبض عليه متلبسا بقرصنة البرامج سيخضع هو وشركته للمحاكمة، بموجب القانون المدني أو الجنائي، وتشمل العقوبات حسب القانون الغرامة المالية مع مصادرة المنتجات والحبس لمدة تصل ثلاث سنوات، بالإضافة إلى معاقبة كل من زور المستندات المعالجة آليًّا أو البيانات المخزنة في ذاكرة الحاسب الآلي، أو على شريط أو أسطوانة ممغنطة، أو غيرها من الوسائل[49].

وأخيراً كما أوضحت بقدر ما تمثله تلك الاتفاقيات والمؤتمرات الدولية والقوانين النموذجية – التي تم تناولها– وبما حوته من مضامين، إلا أن بالإمكان اعتبارها خطوات إيجابية – وإن لم تكن كافية – وتعد أعمال دولية متميزة في مجال الحماية من الجريمة المعلوماتية، وطبيعي أن تأتي متدرجة في تطورها وقوتها، مع تكرار التأكيد بحقيقة القصور في الكثير منها لعدم تضمنها لآليات صريحة في الحماية، ولعل ذلك من البداهة كون الجريمة لا زالت حديثة وفي تطور؛ فهي قيد التطور المتدرج خطورة، وفي الحماية أيضاً، إضافة إلى اعتبار الجماعة الدولية أن العمل والحماية هو عمل وطني داخلي بالأصل، أكثر منه أن يكون عملاً دوليًّا (وهو ما سنتناوله في المبحث الثاني)، إضافةً إلى صعوبة الإجماع بين الدول في قضايا الجرائم المعلوماتية[50].

([47]) د. شمس عبدالله العمرو، " قانون الأونسيترال النموذجي": hnews.net/article/227724

([48])اعتمدت جامعة الدول العربية ما سمي بقانون الامارات الاسترشادي لمكافحة جرائم تقنية المعلومات وما فيه حكمها، نسبة إلى مقدم هذا المقترح وهي دولة الامارات المتحدة، وتم إعتماد هذا القانون النموذجي من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم (459) الدورة 19، بتاريخ 8 أكتوبر 2003م، ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين.

([49]) فريد ناشف، آليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة بليدة، الجزائر، 2013م، ص 101.

من أول الجهود العربية المبذولة من أجل الحماية من جرائم الحاسب الآلي اعتماد مجلس وزراء العدل العرب للقانون الجنائي العربي الموحد كقانون نموذجي بموجب القرار رقم 339 / 1996م، وكانت خطوة هامة في مجال محاربة القرصنة وجرائم الحاسوب.

([50]) تعد الوثائق الاوروبية اقوى الوثائق الإقليمية الخاصة بحماية حقوق الإنسان جملة للأسباب الاتية :

ولذلك كله ينبغي على الأمم المتحدة أن تكمل رؤيتها، وأن تتخذ خطوات محددة نحو تحقيق الهدف في الحماية ومكافحة الجريمة المعلوماتية، وذلك بوضع وتطوير:

1) معايير دولية لأمن المعالجة الآلية للبيانات.
2) اتخاذ تدابير ملائمة لحل إشكالية الاختصاص القضائي التي تثيرها الجرائم المعلوماتية، وهي العابرة للحدود أو ذات الطبيعة الدولية.
3) إبرام اتفاقيات دولية تحتوي على نصوص تنظيم لإجراءات التفتيش والضبط المباشر للجرائم الواقعة، وهي تعبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها، وذلك للمساعدة المتبادلة، مع تأكيد كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدول.

المبحث الثاني
الحماية الوطنية والتعاون الدولي لمكافحة الجريمة المعلوماتية

تنوعت تشريعات الدول فيما يتعلق بحماية الخصوصية ما بين دول أوجدت قوانين خاصة بها، مثل الولايات المتحدة الأمريكية وفرنسا وبريطانيا وكندا والصين ومصر والسعودية، ودولاً اكتفت بالنصوص في القوانين التقليدية كما غالبية دول العالم الثالث – ومنها اليمن– وبلغت بعض الدول في الحماية ومواجهة جرائم الحاسب الآلي والأنترنت إلى النص عليه في دساتيرها مثل النمسا والبرتغال وأسبانيا([51]).

وعليه سنبين في مطلب أول موقف التشريع اليمني، ثم نتطرق في مطلب ثانٍ إلى التعاون الدولي في مكافحة الجريمة المعلوماتية (الأمني والقضائي)، على النحو التالي:

1. شمولية الوثائق الاوروبية لجميع حقوق الإنسان، وايمانها بأهمية هذه الحقوق الإنسان نتيجة لما عانته هذه الدول في الحربين العالميتين.
2. وجود المناخ الملائم الذي يشجع على احترام حقوق الإنسان احتراما فعليا من خلال احترام سيادة القانون وقرارات الاجهزة المعنية.
3. فعالية الرقابة والتنفيذ التي تمت وتتم من لجنة حقوق الإنسان والمحكمة الاوروبية لحقوق الإنسان.
4. حق الفرد في تقديم الشكوى ضد الحكومة.

([51]) BAKKER "R" (computer security hand book) London second edition 1990, p. 291.

أصدرت الولايات المتحدة الأمريكية قانونا لحماية خصوصية برامج الحاسب الآلي لعام 2004م (Computer Software Privacy and Control act of, 2004)، ويجرم هذا القانون أفعالا كالدخول على ملفات الحاسب الآلي دون ترخيص، ويحظر الدخول أو الاطلاع غير المشروع على أجهزة الحاسب الآلي غير المتاحة لاستخدام الجمهور والعائدة ملكيتها للوزارات والمصالح الحكومية، ومن نافلة القول ان قانون الإرهاب الصادر في أكتوبر 2001م وسع من سلطات جهاز استخبارات الأمريكية في عمليات المراقبة الاليكترونية للأفراد سواء في مكان العمل أو في حياتهم الخاصة . (د. نائلة قورة، جرائم الحاسب الآلي الاقتصادية، النهضة العربية، ط 1، 2004م، ص 98).

وفقاً لمؤتمر الأمم المتحدة للتجارة والتنمية (الأونكتاد)، سنّت نسبة 80% من بلدان العالم (156 بلداً) قوانين متعلقة بالجرائم المعلوماتية، وتشمل، من منطقة جنوب غرب آسيا وشمال أفريقيا، مصر وسوريا والكويت والمملكة العربية السعودية والإمارات العربية المتحدة والأردن والعراق وليبيا وتونس والجزائر. إلّا أنّ جودة هذه القوانين ومعاييرها تختلف كثيراً من بلد إلى آخر، علماً أنّ قوانين الجرائم الإلكترونية وحدها لا تكفي لضمان استجابة ملائمة لمشهد التهديدات الرقمية الذي يتطوّر بسرعة.

موقع الأمم المتحدة : https://news.un.org/ar/story/2024/12/1137776

المطلب الأول: الحماية من الجريمة المعلوماتية في التشريع اليمني

بالنظر إلى واقع التشريعات اليمنية[52]، فقد جاءت نصوص **الدستور اليمني** ابتداءً من نص المادة (52) لتقضي بأن: "حرية وسرية المواصلات البريدية والهاتفية والبرقية وكافة وسائل الاتصال مكفولة، ولا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها، أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون، وبأمر قضائي"، ونصت المادة (48) من الدستور: "تكفل الدولة للمواطنين حريتهم الشخصية وتحافظ على كرامتهم وأمنهم. كما لا يجوز مراقبة أي شخص أو التحري عنه إلا وفقا للقانون.."[53].

وبالتمعن في الجريمة المعلوماتية فإنها لا زالت في مهدها على الواقع اليمني، ولكن ذلك لا يعني بأن تؤمن مخاطرها، فقد تصدر موضوعها قانونيًّا، وتصدى لها قانون الجرائم والعقوبات اليمني رقم (12) لسنة 1994م في المادتين (255، 256)، والتي كانت الأولى خاصة بانتهاك حرمة المراسلات، والثانية بالمعاقبة على الاعتداء على حرمة الخصوصية، أما المادة (257) في القانون ذاته فهي خاصة بالتهديد بإذاعة الأسرار الخاصة[54].

ورغم الصياغة القوية للمادة (256) التي اعتبرت كل عدوان يحصل بالقول "بأي جهاز" ، إلا أن جرائم الحاسوب متعددة ومتجددة وذات نوع خاص؛ ولذا فإن

([52]) التشريعات اليمنية تتبع دوماً ما نحاه المشرع المصري؛ إلا أنها هنا تخلفت ولم تواكب تطوره، بالنظر الى التشريع المصري – وهو الأقرب للمقارنة لنا – فانه حقق تقدما كبيراً دستورياً وقانونياً خلال العقدين الماضيين بعمل جملة من القوانين الحماية للمعلوماتية، وإن شابها نوع من النزعة البوليسية، إلا أن الجانب الحمائي الإنساني فيها، والاستقلال القانوني، شيء يذكر وتطور كبير، واكبت فيه مصر التشريعات العالمية والعمل الجماعي الدولي، ومثل هذا تخلف عنه العمل التشريعي في اليمن حيث خلا الحال لدينا من أي تعديل قانوني بشأن الجريمة المعلوماتية، خلاف عن ما يفترض ومأمول وجوده من قانون اليكتروني مستقل، ومن القوانين المصرية التي أوردت نصوصها حماية الفرد من خطر الجريمة المعلوماتية، قانون تنظيم الاتصالات رقم 10 لسنة 2003م قانون مكافحة الإرهاب رقم 94 لسنة 2015م، قانون تنظيم الصحافة والإعلام رقم 180 لسنة 2018م قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م قانون حماية البيانات الشخصية رقم 121 لسنة 2020م قانون الأحوال المدنية رقم 143 لسنة 1994م.

ومن الأعمال المصرية التي حملت آليات ذا طابع عملي وقائي ورقابي؛ ما تضمنه القرار الوزاري رقم(٣٢٧) حول إنشاء إدارة مباحث مكافحة جرائم حاسبات الإنترنت ٢٠٠٥م قانون رقم (١٥) بشأن التوقيع الإلكتروني للعام ٢٠٠٤م، وقبله أنشأت وزارة الداخلية المصرية آلية في هذا الاطار تحت مسمى "إدارة مكافحة جرائم الحاسب الآلي وشبكة المعلومات" التابعة للإدارة العامة للمعلومات والتوثيق، وفقاً للقرار الوزاري رقم (13507) لسنة 2002م، وقد حدد القرار أن للمواطنين الابلاغ عن الجرائم الإلكترونية عبر الوسائل الآتية:

1. الموقع الاكتروني لوزارة الداخلية علي شبكة الانترنت (WWW.Moicgypt.gov.eg)
2. إخطار إدارة مكافحة جرائم الحاسبات وشبكات المعلومات بمقر وزارة الداخلية، سواء بالحضور الشخصي أو الاتصال.
3. يمكن تلقي البلاغات من خلال الخط الساخن (108) والذي تم إنشاؤه لهذا الغرض. (عبد العال الدريبي، محمد صادق اسماعيل، الجرائم الإلكترونية – دراسة قانونية قضائية مقارنة، ط 1، المركز القومي للإصدارات القانونية، 2012م، ص 119).

([53]) وحول آليات التعامل مع الجرائم الإلكترونية ومن أجل عدم المساس بالحقوق والحريات نص الدستور اليمني على ضرورة مراعاة القواعد الإجرائية اللازمة لحماية التهم أو المشتبه به ورتب على عدم مراعاة ذلك البطلان، لذا توجب على العاملين في جمع الاستدلالات التمتع بالإدراك الكامل لهذه التحديات من أجل ضمان حمايتها، وقد نظم القانون كافة الإجراءات اللازمة للسلامة حال مجالها السلوك الإجرائي في مجموعة قواعد قانونية يطلق عليها الشرعية الإجرائية تبدأ من أول وهله وتنتهي بانتهاء العدالة وأصبح يطلق عليها الامن القضائي.

([54]) فمن ناحية تجريم انتهاك حق الانسان في الحماية من الجريمة المعلوماتية؛ فقد نص القانون أنه "يعاقب .. من فتح بغير حق خطاباً مرسلاً إلى الغير، أو احتجز رسالة برقية أو هاتفية .. "، كما نص القانون أن "يعاقب .. كل من اعتدى على حرمة الحياة الخاصة وذلك بأن استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات في مكان خاص أو عن طريق الهاتف، أو التقط، أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص".

إفرادها في قانون خاص هو المفترض، بل ونهيب بالمشرع اليمني ونكرر بلزوم إقرار مشروع قانون وقائي شامل ومستقل، للوقاية من الجريمة المعلوماتية مع تحديد العقوبات؛ إذ مما يلاحظ على النصوص السالفة، أنها لم تبين القصد من إيراد نص "كافة وسائل الاتصال"، وما إذا كانت تشمل أجهزة الحاسوب وما تحتويه.

وفيما يتعلق بالأسرار الموجودة فلم تفصح الأحكام القانونية السابقة إلا عن المكالمات التلفونية فقط، ولا يمكن قبول تعميم النص ليشمل البريد الإلكتروني، كما لا يجوز القياس في النصوص الجزائية بالنسبة لمسائل التجريم([55]).

وفي التهديد بإذاعة الأسرار الخاصة جاء نص المادة (257) بأن:"يعاقب بالحبس مدة لا تزيد على سنتين أو بالغرامة لكل من أذاع أو سهل إذاعة أو استعمل، ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة، أو كان ذلك بغير رضا صاحب الشأن([56]).

ويعد الاحتيال الاليكتروني أحد أشهر أنواع الجرائم الاليكترونية انتشاراً، ويعرف على أنه نوع من أنواع الخِداع والحِيَل التي تتم على شبكة الأنترنت"([57])، كما تأتي جريمة الابتزاز الإلكتروني كأحد أشكال الجريمة الإلكترونية التي تشكل آفة من آفات العصر([58]).

([55]) كما أن النصوص الموجودة في القانون تعاقب الموظفين العاملين في هيئة البريد إذا قاموا بالإطلاع على أسرار المكالمات الهاتفية، بينما في الانترنت قد لا يكون مزود الخدمة من الدولة وإنما شركات خاصة.

([56]) ويعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من هدد بإفشاء أمر من الأمور التي تم الحصول عليها بإحدى الطرق المشار إليها، لحمل شخص على القيام بعمل أو الامتناع عنه، ويعاقب بالحبس مدة لا تزيد على خمس سنوات الموظف العام الذي يرتكب أحد الأفعال المبينة بهذا المادة، اعتماداً على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل منها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها".

([57]) وهي من النماذج للأفعال المجرمة والتي يمكن قيامها من خلال وسائل إلكترونية الجرائم التي تقع على الأموال؛ حيث يعد الحفاظ على الأموال مقصد من مقاصد القانون ولذلك نظم الحماية وتم اعتبارها كأفعال النصب والاحتيال والإبتزاز (استغلال الدعارة) وغسل الأموال، وقد طالت القواعد القانونية لحماية الأموال في السياق الدولي صور عدة أطرافها بلادنا في قانون مكافحة غسل الأموال وتمويل الإرهاب رقم 1 لسنة2010م وتعديلاته بالقانون رقم 17 لسنة 2013م وقوانين عامة وأخرى خاصة. وقد جاء العقاب في القانون اليمني بالمادة (310) من قانون الجرائم والعقوبات، الفصل الثالث بعنوان: "في أكل أموال الناس بالباطل، الاحتيال". بأن: "يعاقب بالحبس مدة لا تزيد على ثلاث سنوات أو بالغرامة من توصل بغير حق إلى الحصول على فائدة مادية لنفسه أو لغيره وذلك بالاستعانة بطريق احتيالية (نصب) أو اتخذ اسم كاذب أو صفة غير صحيحة.

([58]) تعرف جريمة الإبتزاز بأنها: (محاولة تحصيل مكاسب مادية أو معنوية من شخص أو عدة أشخاص سواء طبيعية أو اعتبارية بالإكراه بالتهديد بفضح سر)، وغالباً تبدأ عملية الإبتزاز عن طريق إقامة علاقة صداقة مع الشخص المستهدف، ثم يتم الانتقال إلى مرحلة التواصل عن طريق برامج المحادثات المرئية (Video conferencing) ، ليقوم بعد ذلك المبتز بإستدراج الضحية وتسجيل المحادثة التي تحتوي على محتوى مسيء وفاضح للضحية، ثم يقوم أخيراً بتهديده وإبتزازه بطلب تحويل مبالغ مالية أو تسريب معلومات سرية، وقد تصل درجة الإبتزاز في بعض الحالات إلى إسناد أوامر مخلة بالشرف والأعراف والتقاليد مستغلاً بذلك إستسلام الضحية وجهله بالأساليب المتبعة للتعامل مع مثل هذه الحالات، وفي حادثة شهيرة في نوفمبر 2022، أطلقت الناشطة الإنسانية، سارة علوان، النار على نفسها، في محاولة للانتحار، بعد أن تعرضت للإبتزاز والتهديد بنشر صورها، كما أقدمت فتاة في إحدى مديريات محافظة تعز على الانتحار شنقا بعد تعرضها لعملية إبتزاز إلكتروني . (القاضي أنيس صالح جمعان، التصنيف القانوني لجرائم الإبتزاز الإلكتروني، مرجع سابق).
وقد عاقبت عليها المادة (313) عقوبات بقولها: "يعاقب بالحبس مدة لا تتجاوز خمس سنوات أو بالغرامة كل من يبعث قصداً في نفس شخص الخوف من الإضرار به أو بأي شخص آخر يهمه أمره ويحمله بذلك وبسوء قصد على أن يسلمه أو يسلم أي شخص آخر أي مال أو سند قانوني أو أي شيء يوقع عليه بإمضاء أو ختم يمكن تحويله إلى سند قانوني".

وممّا سبق يتضح بأن نصوص قانون العقوبات اليمني غير دقيق بالمعنى القانوني المطلوب للفصل في قضايا الحاسوب والجرائم المعلوماتية الخطيرة والمتجددة([59]).

وفي ضوء القصور والغموض في التشريعي اليمني فيما يخص حماية حق الإنسان من الجريمة المعلوماتية، يمكننا القول: إن هناك العديد من الإشكالات الشرعية والقانونية التي تواجه رجال العدالة الجنائية في اليمن، تتمثل في عدم وجود تشريع جنائي خاص بالجرائم المعلوماتية، ينظم جمع الاستدلالات والتحقيق في الجرائم المعلوماتية وطرق إثباتها؛ ولذا فلا مناص بعدها أمام القضاة وفي ظل تزايد قضايا الابتزاز الإلكتروني التي تُعرض أمامهم إلا بالرجوع إلى نصوص وأحكام القانون اليمني؛ خصوصاً قانون الجرائم والعقوبات في المواد (245- 255 - 256- 257- 313)، والقانون رقم (13) لسنة 1994م بشأن الإجراءات الجزائية، والقانون رقم (40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وكل ذلك يؤدي بلا شك إلى المساس بمبدأ الشرعية الجنائية، ومبدأ التفسير الضيق للنص الجنائي، بحيث يعرض إجراءات الاستدلال والتحقيق وحتى المحاكمة لعورات قانونية تشوبها، وبالتالي إمكانية الطعن فيها؛ مما يؤدي بالنتيجة إلى بطلانها.

وبالنظر في القانون رقم (٢١) لسنة ١٩٩٢م بشأن الإثبات، فإن الواقع العملي أثبت أن المحاكم اليمنية تعتبر وسائل التواصل الإلكتروني والاجتماعي، إحدى وسائل إثبات الجريمة على الرغم من أن قانون الإثبات يعتبرها من القرائن التي تحتاج للتعزيز والدعم من قبل دليل آخر لقبولها، كعرضها على الجاني للإقرار بصحتها؛ لتعتبره المحكمة دليلًا كاملًا بالاستناد لإقراره، لا بالاستناد لقوة الدليل الإلكتروني نفسه، أما إذا أنكر الجاني ما عرض عليه في الوسيلة الإلكترونية، فيتم عرض هذا الدليل على "خبير فني تقني"؛ ليحدد صحة هذا الدليل من عدمه ([60])، ولعل هذا العمل أكثر استخداماً لدي القضاء بنيابة ومحاكم الصحافة، حيث إن أغلب الاعتداء بالنشر يتم اليكترونيًّا.

ومن القوانين اليمنية التي تناولت جوانب حمائية من الجريمة المعلوماتية الاليكترونية جاء القانون رقم (64) لسنة 1991م بشأن البريد والتوفير البريدي، الذي جاء ضمن المادة (2 / الفقرة – ل) منه أن:" البعائث البريدية: تشمل الرسائل العادية والصوتية والإلكترونية والفواتير والمستندات والبطاقات البريدية والمطبوعات ومكتوبات المكفوفين..." ([61]). ورغم تقدم ألفاظ التقنين بتناول مصطلحات الرسائل الصوتية

([59]) مع التأكيد حقيقة أن أجهزة إنفاذ القانون عادة تتعامل مع الشكاوى حسب الإجراءات المنصوص عليها في القانون، وأن الخلل ليس في أجهزة القضاء، وإنما في قصور التشريعات، وبالتالي فلا تقاعس من أجهزة القضاء وتفاعلها مع الشكاوى المرفوعة إليها، خاصة إذا كانت الضحية امرأة أو فتاة؛ نظراً لحساسية الأمر، وضعف الضحية في كيفية التعامل مع المُبْتَز والتهديدات التي تتلاقها.

([60]) المستشار/ د. صالح عبدالله المرفدي، الجرائم المرتكبة على وسائل التواصل الاجتماعي:
https://www.aden-tm.net/news/270205

تتمثل طرق الاثبات العادية في الجريمة المعلوماتية بالأدلة الكتابية، الشهادة، القرائن، الاعتراف، اليمين، المعاينة والخبرة، الحيازة.

([61]) وحول الامتياز البريدي وسرية المراسلات ورد في المادة (5 /3/ ب): "يكون للهيئة دون غيرها القيام بما يلي .. قبول وجمع وتوزيع ونقل مختلف البعائث البريدية إلى جميع الجهات وبمختلف الطرق والوسائل ويشمل ذلك الرسائل المنقولة بوسائط النقل الإلكتروني للجمهور"، وهنا تصور متقدم من المشرع وسبق يحسب بذكر عملية النقل الاليكتروني وكنوع من الالتزام بالحماية والمسئولية.

والإلكترونية، والنقل والإليكتروني، إلا أنه لا يوجد تعريف أو نص حمائي أو عقابي صريح حيال المخالفة أو الانتهاك لقيام الجريمة المعلوماتية[62].

وجاء في القانون رقم (38) لسنة 1991م بشأن الاتصالات السلكية واللاسلكية، ووفقاً للمادة (18/5) فإنه: "لا تجوز بأي حال رقابة المحادثات والرسائل إلا بإذن خطي مسبق من سلطات التحقيق المختصة، وذلك وفقا لأحكام قانون الإجراءات الجزائية وبواسطة الوزير"[63].

أما قانون الصحافة والمطبوعات اليمني رقم (٢٥) لسنة ١٩٩٠م، فتضمن – فيما يخص عقوبة التشهير – نص المادة (103) التي تقضي بأن: "يلتزم كل من العاملين في الصحافة المقروءة والمسموعة والمرئية ... بالامتناع عن طباعة ونشر وتداول واذاعة ما يلي: "1. ما يؤدي إلى الإخلال بالآداب العامة، وما يمس كرامة الشخص والحريات الشخصية، بهدف الترويج والتشهير الشخصي، 2. الإعلانات المتضمنة عبارات أو صورًا تتنافى مع القيم الإسلامية والآداب العامة، أو قذف وتشويه سمعة الأشخاص أو الاعتداء على حقوق الغير، أو تضليل الجماهير"[64].

كما جاء القانون اليمني رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات، في حماية الخصوصية ما أفادت به المادة (50) بأنه : "لا يجوز لأي جهة جمع أو معالجة أو حفظ أو استخدام البيانات الشخصية للمواطن، خلافاً للدستور والقوانين النافذة"[65].

وثمة إبداع تشريعي عالمي إنساني في قانون حق الحصول على المعلومات في أنه جعل الحماية شاملة

---

(62) بالنظر إلى تجارب الدول العربية فان الإمارات تعد أول دولة عربية تصدر قانونا مختصا في مكافحة جرائم المعلومات ؛ حيث صدر هذا القانون الاتحادي رقم (2) لعام 2006م في شأن مكافحة جرائم تقنية المعلومات، كما أقرت السعودية نظامي التعاملات الاليكترونية ومكافحة الجرائم المعلوماتية بقرار مجلس الوزراء رقم (80) 1428/3/7هـ.، والذي يهدف إلى ضبط التعاملات والتوقيعات الاليكترونية، وتنظيمها، وتوفير إطار نظامي لها نظام التعاملات الاليكترونية، ويعد قانون الجزاء العماني أول قانون عربي تطرق إلى مواجهة الجرائم المعلوماتية من خلال التعديل الذي تم على قانون الجزاء العماني الصادر عام 1974م بموجب المرسوم السلطاني رقم 2001/72م، ومن ضمن هذه التعديلات إضافة الفصل الثاني مكرر على الباب السابع تحت عنوان جرائم الحاسب الآلي.

(63) ونصت (21/5) أيضاً أنه "يحظر حظراً باتاً استعمال الأجهزة اللاسلكية المرخص بها في الأغراض التالية: أ– التقاط مراسلات لم يسمح بالتقاطها، وفي حالة التقاطها من غير عمد لا يجوز بأي حال تسجيلها إلى الغير أو استعمالها لأي غرض كان. ج – تعمد إرسال إشارات أو رسائل أو صور مخالفة للشريعة الإسلامية وللنظام العام أو النظام الاجتماعي أو الآداب أو أمن الدولة وسلامتها".

(64) التشهير: هو تصريح مكتوب أو مطبوع عبر وسائل الصحافة, يقصد به إيذاء سمعة شخص ما، باستخدام الصور والإشارات أو بث الأخبار, ويمكن أن يكون المذياع والتلفاز من سائل نقل هذه الأشياء المسيئة للسمعة، وقد يكون إقدام شخص طبيعي أو معنوي على إصدار كلام مكتوب باليد أو مطبوع بالآلة يتضمن تهجماً على أحد الاشخاص أو أحدى المؤسسات،يمس سمعتها بهدف التشويه والتشهير بها.

يشار إلى ان العاصمة اليمنية المؤقتة عدن شهدت بداية مارس 2024م، افتتاح أول شعبة متخصصة في مكافحة الجرائم الإلكترونية؛ للتعامل مع الشكاوى المتزايدة والفصل في القضايا المنظورة، بدءًا من مايو/ أيار المقبل، بعد تدريب موظفين على التعامل معها.

(65) احتوى القانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات على (66) مادة موزعة على ستة أبواب، وتضمن فيما يهمنا بشأن خصوصية المعلومات وحظر إفشائها ما ورد في المادة (25) القاضية أن: "على الموظف المختص رفض أي طلب حصول على المعلومات إذا كانت تحتوي على:

أ- المعلومات المتوقّع، في حال الإفصاح عنها، تعريض حياة فرد ما أو سلامته الجسدية للخطر.

ب- البيانات الشخصية، التي من شأن الإفصاح عنها، أن يشكل انتهاكا غير منطقيا لخصوصيات الفرد، ما لم تكن البيانات الشخصية متّصلة بواجب أو وظيفة أو منصب عام يشغله هذا الفرد".

للوطني وغيره، وذلك في مواجهة الدول الأخرى؛ ولم يجعل الحماية للوطني وحسب، وقد تأتى ذلك بنص المادة (53) من أنه: "لا يجوز تقديم بيانات شخصية لأي دولة أو جهة خارجية أخرى لا تتوفر لديها ضمانات قانونية مماثلة لحماية الخصوصية"[66].

وأخيراً نشير إلى الأهم، وهو القانون اليمني رقم (40) لسنة 2006م، بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، والذي يعالج هذه الجرائم بشكل جزئي، فقد جاء في القانون المشار إليه بنص المادة (10) التي تقضي بأن: "يكون للسجل الإلكتروني والعقد الإلكتروني ورسالة البيانات والمعلومات الإلكترونية والتوقيع الإلكتروني نفس الآثار القانونية المترتبة على الوثائق والمستندات والتوقيعات الخطية من حيث إلزامها لأطرافها أو حجيتها في الإثبات"[67].

ومن أهم مبادئ حماية البيئة الإلكترونية في قانون أنظمة الدفع هو تجريم أي نتيجة إجرامية تكون قد تمت بوسيلة إلكترونية، وهذا ما يتضح في نص المادة (41) في القانون المذكور – وذلك عوضاً عن انعدام النص العقابي بقانون الجرائم والعقوبات– والتي تعتبر من أكثر المواد التي يعود لها القاضي اليمني في تكييفه للقضية، ومن ثم بناء الحكم، ونصت بأن: "يعاقب كل من يرتكب فعلاً يشكل جريمةً بموجب أحكام القوانين النافذة بواسطة استخدام الوسائل الإلكترونية بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنة، أو بغرامة لا تقل عن ثلاثمائة ألف ريال ولا تزيد على مليون ريال".

ومع النص سالف الذكر فإننا ندعو إلى اعتبار مجرد قيام الفعل المجرَم بوسيلة إلكترونية ضمن تقدير الظرف المشدد؛ وذلك تطبيقاً لنص المادة (37) بأنه: "مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر نافذ يعاقب كل من يخالف أحكام هذا القانون بالعقوبات الواردة في هذا الفصل".

نخلص إجمالاً إلى أننا نعيش في اليمن في ظل وضع يمكن القول عنه: إننا أمام فراغ أو قصور تشريعي لمواجهة الجرائم المعلوماتية؛ ولهذا نقترح على المشرع اليمني العمل على إصدار قانون مستقل لحماية البيانات المعلوماتية، وليس مجرد إضافة نصوص مستقلة منظمة في قانون العقوبات تعاقب عن حالات الاختراق المكونة للجريمة المعلوماتية[68].

([66]) وفي ذات القانون نصت المادة (54) أنه: "لا يجوز لأي جهة استخدام البيانات الشخصية في غير الأغراض التي جمعت من أجلها"، كما جاء في تقنين صريح تضمنه نص المادة (56) أن: "كل جهة تحتفظ ببيانات شخصية تكون مسئولة مسؤولية تامة عن حماية هذه البيانات وعليها وضع بيان معتمد للخصوصية يبين نظم وإجراءات التعامل مع سرية البيانات الشخصية ويكون متاح للإطلاع".

([67]) وعقابياً جاء في المادة (38): 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، مع إرجاع المبالغ التي قام بالاستيلاء أو الحصول عليها أو سهل للغير الحصول عليها.

([68]) نشير أخيراً إلى أهم الاعمال القانونية التي قامت بها اليمن، مما صدر عن المشرع اليمني من النصوص القانونية التي تناولت مباشرة أو بالاشارة إلى الجريمة المعلوماتية في الأحكام والحماية منها، أو الموقف من الاتفاقيات الدولية بهذا الصدد، وكل ذلك كما يلي:

1 – قانون رقم (٢٥) لسنة ١٩٩٠ م بشأن الصحافة والمطبوعات 2 – القانون رقم (38) لسنة 1991م للاتصالات السلكية واللاسلكية والمعدل بالقانون (33) 1996م 3 – قانون رقم (64) لسنة 1991م بشأن البريد والتوفير البريدي 4 – القانون رقم (٢١) لسنة ١٩٩٢م بشأن الإثبات (وتعديلاته) 5 – قانون الجرائم والعقوبات اليمني رقم (12) لسنة 1994 م وتعديلاته. 6 – القانون رقم (13) لسنة 1994م بشأن الإجراءات الجزائية. 7 – قانون الوثائق رقم (21) لسنة 2002 م. 8 – قانون رقم (35) بشأن

المطلب الثاني : التعاون الدولي في مكافحة الجريمة المعلوماتية

نظراً لما تمثله الجرائم المعلوماتية من خطورة على المجتمع الدولي ككل، ولأن مرتكبي هذه الجرائم ينتمون إلى جنسيات متنوعة وبلدان مختلفة، فإن الأمر يتطلب التعاون بين مختلف الدول والهيئات لمكافحة هذا النوع من الجرائم، وفيما يلي سنتناول التعاون الأمني ودور المنظمة الدولية للشرطة الجنائية (الإنتربول)، وتسليم المجرمين، ثم المساعدة القضائية الدولية، ومن ثم معوقات التعاون الدولي، وذلك على النحو الآتي:

أولاً: التعاون الأمني: مع تميز الجرائم المعلوماتية بخاصية العالمية، وكونها عابرة للحدود فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بالاتصال المباشر بين أجهزة الشرطة في الدول، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها.

وكعمل دولي متكامل جاءت المنظمة الدولية للشرطة الجنائية "الإنتربول"؛ International Criminal Police Commission (ICPO) ، بهدف التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعّال في مكافحة الجريمة، بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة(69)، ومن ثم يقوم الإنتربول بعملية ملاحقة مرتكبي الجرائم وجرائم شبكة الإنترنت خاصة، عن طريق تعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي والأنظمة المعلوماتية وشبكات الاتصال بحثًا عن ما قد تحويه من أدلة وبراهين عن

مكافحة غسيل الأموال لسنة 2003م. 9 – قانون الأسماء التجارية رقم (20) لسنة 2003 م. 10– القانون رقم (40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية 11 – قانون حماية المستهلك رقم (45) لسنة 2008 م. 12 – قانون العلامات التجارية والمؤشرات الجغرافية رقم (23) لسنة 2010 م. 13– قانون مكافحة غسل الأموال وتمويل الإرهاب (1) 2010م وتعديلاته بالقانون (17) 2013م 14 – القانون رقم (21) لسنة 2010 م بشأن حماية الإنتاج الوطني من الأثار الناجمة عن الممارسات الضارة في التجارة الدولية 15 – القانون رقم (2) 2011 م بشأن براءة الاختراع ونماذج المنفعة. 16 – القانون رقم (13) لسنة 2012 م بشأن حق الحصول على المعلومات ولائحته التنفيذية. 17 – القانون رقم (15) لسنة 2012 م بشأن حماية حق المؤلف والحقو المجاورة. 18 – القانون رقم (20) لسنة 2020 م بشأن تنظيم الصناعة. 19 – مشروع القانون الخاص بمكافحة جرائم تقنية المعلومات لسنة 2020 م. 20 – الانضمام للاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2018م 21 – الانضمام إلى المنظمة العالمية لحماية حقوق الملكية الفكرية (الويبو / 1967). 22 – الانضمام إلى اتفاقية باريس لحماية الملكية الصناعية (2006 م) .

كل هذه الأعمال تمثل خطوات ايجابية طيبة في سبيل الانتقال إلى العمل الأهم وهو اصدار قانون خاص بالجرائم المعلوماتية لتأكيد المواكبة للمواثيق الدولية وتشريعات الدول المعاصرة والاستفادة من كل مضامينها.

(69) Malcom Anderson: " Policing the world: Interpol the Politics of International Police Co– Operation " , Clarendon press.Oxford,1989,p 168–185

أسس الأنتربول، وهو أكبر منظمة شرطية في العالم، عام 1923م، وتقع الأمانة العامة للأنتربول في ليون بفرنسا، ومهمته تتمثل في تقديم المساعدة إلى أجهزة إنفاذ القانون في بلدانه الأعضاء ال 192 لمكافحة جميع أشكال الإجرام عبر الوطني , وللأنتربول بنى تحتية متطورة للإسناد الفني والميداني, تمكين قوى الشرطة في سائر أنحاء العالم من مواجهة التحديات الإجرامية المتنامية في القرن الحادي والعشرين.

وتركز المنظمة اهتمامها على مجالات حماية من جرائم أعطتها الأولوية وهي: الفساد والمخدرات والإجرام المنظم والإجرام المالي والمرتبط بالتكنولوجيا المتقدمة والمجرمون الفارون وتهديد السلامة العامة والإرهاب والاتجار في البشر.

(د. محمود شريف بسيوني "المحكمة الجنائية الدولية مدخل لدراسة أحكام وآليات الإنفاذ الوطني للنظام الأساسي" دار الشروق الطبعة الأولى 2004م، ص 143).

ارتكاب الجريمة المعلوماتية([70])، ولا شك أن العمل الدولي الجماعي، والتعاون من خلال تفعيل عمل الإنتربول الدولي، يساعد في العدالة من محترفي الإجرام الإليكتروني، ومن ثم إعادة الحقوق الإنسانية المادية والمعنوية.

كما يعتبر تسليم المجرمين من أشكال التعاون الأمني بين الدول في مكافحة الجريمة وحماية المجتمعات من المخلين بأمنها واستقرارها، وحتى لا يبقى أولئك العابثين بمنأى عن العقاب([71]).

ويتم تسليم المطلوبين بناءً على نظام محدد بموجب القوانين الداخلية (الوطنية) التي تنظم تسليم المجرمين، أو العرف الدولي أو الاتفاقيات الدولية، والتي من صورها:

أ – الاتفاقية الثنائية التي تنظم مسألة تسليم المجرمين بين دولتين؛ كما هي بين اليمن وكثير من الدول العربية والعالمية.

ب – الاتفاقية متعددة الأطراف (الإقليمية) بشأن تسليم المجرمين، ومن ذلك اتفاقية الدول العربية لتسليم المجرمين لعام 1952م، اتفاقية الرياض العربية للتعاون القضائي لعام 1983م، والاتفاقية الأمنية الخليجية لعام 1994م.

ج – الاتفاقيات الدولية العامة، مثل معاهدة الأمم المتحدة النموذجية لتسليم المجرمين لعام 1990م، التي مثلت إطارا يساعد الدول التي بصدد التفاوض على اتفاقيات التسليم الثنائية، وتتكون هذه الاتفاقية من (18) مادة إضافة إلى ملحق صدر لها عام 1997م تضمن بعض الأحكام التكميلية، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000م([72]).

ثانياً : المساعدة القضائية الدولية ([73]): وتتخذ المساعدة القضائية في المجال الجنائي صورًا منها:

1 – تبادل المعلومات: ويشمل تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية، وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة([74]).

([70]) موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة:https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html.

على المستوى العربي قام مجلس وزراء الداخلية العرب بانشاء المكتب العربي للشرطة الجنائية، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين, ومقره دمشق سابقاً والرياض حالياً.

([71]) تسليم المجرمين يعني: قيام دولة ما بتسليم شخص ما موجودا في إقليمها إلى دولة أخرى، بناءً على طلبها بغرض محاكمته عن جريمة نسب إليه ارتكابها أو لتنفيذ حكم صادر ضده من محاكمها.

هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، مصر، 2005، ص 69

([72]) قرار الجمعية العامة للأمم المتحدة، وثيقة A/RES/SS/25_ بتاريخ 2000/1/8م.

([73]) تعرف المساعدة القضائية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم.

(د. سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراة، كلية الحقوق / جامعة عين شمس، 1997م، ص 425).

([74]) أحمد فاروق زاهر، الجريمة المنظمة / ماهيتها، خصائصها، أركانها، مركز الد راسات والبحوث / أكاديمية نايف العربية للعلوم الأمنية، الرياض،،

وفي هذا العمل يكون الجانب وقائيا مفيداً ربما بقطع طريق اكتمال الجريمة قبل اتمامها.

2 – **نقل الإجراءات:** قيام دولة ما –بناء على اتفاقية أو معاهدة– باتخاذ إجراءات جنائية، وهي بصدد جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الدولة، متى ما توافرت شروط معينة([75]).

وتفيد هذه الجزئية في أن طبيعة الجريمة قابلة للإخفاء والمحو من الوجود في لحظات، وبالتالي يمكن الاستدراك بالانتقال في التحقيق والضبط إلى المكان الرئيس للجريمة ومرتكبها.

3 – **الإنابة القضائية الدولية:** ويقصد 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، وعادة – وكما هو معهود – يتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية([76]).

ثالثاً: معوقات التعاون الدولي([77]):

1. عدم وجود نشاط موحد للنشاط الإجرامي: ويرجع ذلك إلى أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات، وبالتالي اختلاف السياسة التشريعية من مجتمع لآخر([78]).
2. تنوع واختلاف النظم القانونية الإجرائية: فما قد يكون قانونيًّا ومشروعًا في دولة معينة، قد لا يكون مشروعًا في دولة أخرى، ومن ذلك طرق جمع الاستدلالات.
3. عدم وجود قنوات اتصال: فعدم وجود هذا النظام يعني عدم القدرة على جمع الأدلة والمعلومات العملية التي غالبًا ما تكون مفيدة في التصدي لجرائم معينة ولمجرمين معينين([79]).
4. مشكلة الاختصاص في الجرائم المتعلقة بالأنترنت: لاتسام الجريمة المعلوماتية بأنها عابرة للحدود فإن ارتكاب جريمة في إقليم دولة معينة

2007، ص 387، وهي ذات المادة (5) من اتفاقية الرياض العربية للتعاون القضائي 1983م.

([75]) أقرت العديد من الاتفاقيات الدولية والإقليمية الانابة القضائية؛ أهمها معاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية، واتفاقية الرياض العربية للتعاون القضائي / الرياض 1993/4/6م، ومعاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي ؛ والتي صدرت واعتمدت عام 1999م من قبل مؤتمر وزراء خارجية دول المنظمة في اجتماعهم المنعقد في أوغادوغو 1999م، والنموذج الإرشادي لاتفاقية التعاون القانوني والقضائي الصادر عن مجلس التعاون الخليجي، الكويت2013م، ومعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية والتي اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14م، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية 2000م. (د. محمود إبراهيم غازي، مرجع سابق، ص 83).

([76]) أمجد عبد الكريم سلامه، فقه المرافعات المدنية الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2000، ص 98.

ولأهمية الإنابة القضائية، أبرمت العديد من الاتفاقيات الدولية الجديدة بهذا الصدد، والتي ساهمت في اختصار الوقت والإجراءات عن طريق الاتصال المباشر بين السلطات المعنية بالتحقيق، ومن ذلك معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لعام 1999م، واتفاقية الرياض العربية للتعاون القضائي لعام 1983م، واتفاقية "شينغين" لعام 1990م الخاصة باستخدام الاتصالات المباشرة بين السلطات القضائية في الدول الأطراف، واتفاقية الأمم المتحدة لمكافحة الفساد.

([77]) د. محمود إبراهيم غازي،مرجع سابق، ص46.

([78]) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2009م، ص 102.

([79]) د. جميل عبد الباقي الصغير، الجوانب الاجرائية المتعلقة بالانترنت، دار النهضة العربية 2018م، ص 72.

من قبل أجنبي قد يؤدي لاحتمالات أن تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولى استنادًا إلى مبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى، فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية([80]).

5. التجريم المزدوج: يعتبر من أهم الشروط الخاصة بنظام تسليم المجرمين، ونصت عليه أغلب التشريعات الوطنية والصكوك الدولية المعنية بتسليم المجرمين([81]).
6. الصعوبات الخاصة بالمساعدات القضائية الدولية: عادة ما تتم الإنابات القضائية الدولية بالطرق الدبلوماسية؛ ولهذا تتسم بالبطء والتعقيد، وهو ما يتعارض مع طبيعة الأنترنت وما يتميز به من سرعة، إضافة إلى مشاكل نقص الموظفين المدربين مع الصعوبات اللغوية وغير ذلك([82]).
7. الصعوبات الخاصة بالتعاون الدولي في مجال التدريب: سواء من خلال وجود الفوارق الفردية، أو عدم وجود أي خلفية لكثير من الإداريين في هذا المجال، وعلى النظير وجود خبرات على درجة كبيرة من المعرفة([83]).

وبالنظر إلى الجهود الوطنية سواء في التشريعات، أو من خلال التعاون بين الدول، فإنها لا تزال قاصرة عن توفير الحماية من الجريمة المعلوماتية، ولن تكتمل الحماية إلا من خلال العمل على كافة الأصعدة الوطنية، تشريعيًّا وسياسات عملية، خصوصاً ونحن أمام جريمة نوعية متطورة ومتجددة، ومحترفيها من الذكاء والخطورة بمكان، ما تصبح معه المواكبة ضرورة في كل أعمال الدولة أمراً حتميًّا، ومن ثَم يأتي التعاون الدولي – والثنائي خاصة – وذلك حماية للمجتمع، وسلامة خصوصياته، وكل ما يمكن أن يمس كيان الفرد فيه كإنسان ماديًّا أو معنويًّا.

الخاتمة

نخلص في نهاية هذه الدراسة عن "حق الإنسان في الحماية من الجريمة المعلوماتية في القانون الدولي والقانون اليمني"، إلى مجموعة من النتائج والتوصيات على النحو الآتي:

- **النتائج**:

1. اهتم المجتمع الدولي بحياة الإنسان كفرد وحياته الخاصة بفرض الحماية القانونية له، على الصعيد الدولي أو الوطني؛ إذْ تم التأكيد على هذه الحماية في الاتفاقيات الدولية، وكانت موضوعاً لبحث مستفيض في العديد من المؤتمرات، كما حرصت جميع المنظمات والهيئات الدولية والإقليمية على بسط الحماية اللازمة له، وفي مقدمتها

([80]) هذه المعايير الثلاثة هي مكان القبض على المتهم، ومكان وقوع الجريمة، أو محل إقامة المتهم.

([81]) تأتي الصعوبة في أن معظم الدول لا تجرم هذه الجرائم، إضافة إلى صعوبة تطبيق النصوص التقليدية لدى الدولة المطلوب منها التسليم إن كان بالإمكان أن تنطبق على الجرائم المتعلقة بشبكة الانترنت من عدمه، وهو ما يعوق تطبيق الاتفاقيات الدولية في مجال تسليم المجرمين، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المتعلقة بالانترنت د. جميل عبد الباقي الصغير، المرجع السابق، ص 91.

([82]) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، مرجع سابق، ص 125 .

([83]) د. جميل عبد الباقي الصغير، الجوانب الاجرائية المتعلقة بالانترنت، مرجع سابق، ص 113.

الأمم المتحدة.

2. أدى التطور التقني في الحاسب الآلي وشبكة الأنترنت، إلى نشوء تقنيات جديدة تستخدم في انتهاك خصوصية الأفراد، كما أدى إلى ظهور صور جديدة للجرائم، وهي الجرائم المعلوماتية، وهذه الصور لا تنطبق مع الجرائم في القوانين التقليدية.

3. تثير جرائم الحاسب الآلي مشاكل وصعوبات تتعلق بإقامة المسؤولية الجنائية بحق مرتكبيها ومعاقبتهم، حيث صعوبة تحصيل وإثبات الدليل، ومن ثم مسائل الاختصاص القضائي والقانون الواجب التطبيق، وهو ما يعانيه القاضي اليمني في التكييف وبناء الحكم.

4. إن انضمام أي دولة للاتفاقيات الدولية لحقوق الإنسان يفترض معه أن يؤدي إلى مبادرة المشرع الوطني بإصدار التشريعات الموائمة للاتفاقيات، سواء بتعديل ما هو سارٍ فعلا من تشريعات أو استحداث مواد أو قوانين جديدة.

5. يعد العمل الأوروبي هو الأنموذج والأكمل عالميًّا في مكافحة الجريمة المعلوماتية، سواء من خلال الاتفاقيات أو المؤتمرات او القوانين النموذجية، واتفاقية بودابست 2001م شاهدة على ذلك.

6. يعد التعاون الدولي مظهراً مُهمًّا وآلية ناجعة للحماية من الجريمة المعلوماتية، سواء كان استجابة لمضمون الاتفاقيات الدولية، وما تحمله من أحكام ودعوة الدول للانضمام لها، ولإصدار قوانين حمائية وطنية خاصة بهذه الجريمة، أو من خلال التعاون القضائي والامني، الثنائي أو الجماعي.

7. مع حقيقة أن العمل الدولي الجماعي لا زال قاصراً، إلا أن صدور الاتفاقية الدولية لمكافحة الجريمة المعلوماتية في 2024/12/24م، أمر يبشر بمزيد من التفاعل الدولي في مجال مكافحة الجريمة المعلوماتية.

- **التوصيات**:

1) يوصي الباحث بأنه يجدر بالمشرع اليمني على وجه اللزوم إيجاد تشريع خاص بالجريمة المعلوماتية – كما في الفرنسي والمصري وغيرهما – ينظم فيه بالتجريم والعقوبة لكل حالات إنتهاك حرمة حياة الفرد الخاصة والعملية بواسطة الأجهزة الإليكترونية والإنترنت.

2) نهيب بالقضاء اليمني التشدد في الإجراءات القضائية للحد من الاعتداء على حياة الفرد الخاصة، وذلك بالأمر العاجل ابتداءً بوقف النشر أو الحذف، أو حتى المصادرة بحق المطبوعات، وكل الأعمال الماسة بهذا الحق حفاظاً على خصوصية حياة الفرد.

3) نوصي المشرع اليمني بالنص على عدم تقادم الدعوى الجنائية أو المدنية بحق جرائم الاعتداء على حرمة الحياة الخاصة للإنسان، ومنها الجرائم الإليكترونية، وذلك ردعاً وزجراً لكل مرتكب لهذه الجريمة مهما طال الزمن.

4) يوصي الباحث الحكومة اليمنية بإنشاء مراكز متخصصة لتلقي الشكاوى المتعلقة بجرائم الإنترنت، – أسوة بالعمل المصري – وأن يمنح أعضاء هذه المراكز، بعد تأهيلهم، صفة

الضبطية القضائية، لتكون مهمتهم جمع الاستدلالات في الجرائم الإلكترونية.

5) العمل على تحديث مناهج المعهد العالي للقضاء لتتضمن البرامج التقنية في مجال التحقيق في الجرائم المعلوماتية، مع تأهيل المحققين في النيابة والقضاة، مع بيان أهمية التوعية بأهمية وحرمة خصوصية الإنسان، وإحاطتهم بالنصوص والمبادئ الدولية الحديثة، وما بلغته الأعمال العالمية المتعلقة بحقوق الإنسان بهذا الشأن.

6) العمل على نشر ثقافة حقوق الإنسان وحرمة الحياة الخاصة بين المواطنين، ولا سيما الشباب ابتداءً من التوعية المبكرة في المدارس من مخاطر التعامل مع المواقع السيئة على شبكة الأنترنت، مع ضرورة العمل على تقرير تدريس مادة حقوق الإنسان في كافة كليات الدراسة الجامعية.

7) ضرورة أن تتحد الجهود الدولية لتحديد أطر التعاون في مجال مكافحة الجريمة المعلوماتية، وذلك بعقد اتفاقيات دولية، مع الدعوة إلى بذل الجهود لتحقيق التعاون الدولي، الثنائي والإقليمي والجماعي، وتبادل الخبرات للاستفادة من التجارب الواقعية للدول حول الجرائم المعلوماتية.

المصادر والمراجـع

الكتب القانونية المتخصصة:

[1] د. إبراهيم أحمد الصعيدي، نظام التشغيل الإليكتروني للبيانات، مطبعة المعرفة، 1981م.

[2] د. أحمد خليفة الملط، الجرائم المعلوماتية، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية،2005م.

[3] أحمد فاروق زاهر، الجريمة المنظمة ماهيتها، خصائصها، أركانها، مركز الد راسات والبحوث، أكاديمية نايف العربية للعلوم الأمنية، الرياض،، 2007م.

[4] د. أسامة عبد الله قايد، الحماية الجنائية وبنوك المعلومات، دار النهضة العربية، ط 3، 2008م.

[5] السيد أبو الخير، نصوص المواثيق الدولية والإعلانات والاتفاقيات لحقوق الإنسان، إيتراك للنشر والتوزيع – القاهرة، 2005م.

[6] أمجد عبد الكريم سلامه، فقه المرافعات المدنية الدولية، ط1، دار النهضة العربية، القاهرة، 2000م.

[7] د. أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، ط 1، مكتبة الوفاء القانونية، مصر، 2011م.

[8] د. بولين انطونيوس ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة – منشورات الحلبي الحقوقية، 2009م.

[9] د. جميل عبد الباقي الصغير، الجوانب الاجرائية المتعلقة بالأنترنت، دار النهضة، 2018م.

[10] عبد العال الديربي، محمد صادق اسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة، ط 1، المركز القومي للإصدارات القانونية، 2012م.

[11] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، القاهرة، 2009م.

[12] د. عمر أبو الفتوح الحمامي، الحماية الجنائية للمعلومات المسجلة إليكترونيًّا، دراسة مقارنة، دار النهضة العربية، 2010م .

[13] د. عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، النهضة العربية، 2004م.

[14] د. عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ط 2، 2007م

[15] د. فاروق محمد الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، ط 1، دار الجامعة الجديدة، 2002م

[16] د. فؤاد بن صغير، التجارة الدولية، مطبعة فضالة المغرب، الطبعة الأولى، 2000م.

[17] د. محمد الأمين ومحسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة أكاديمية نايف العربية للعلوم الأمنية الرياض، ط 1، 1998م.

[18] د. محمد امين الشوابكة، جرائم الحاسوب والانترنت/ الجريمة المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، ط 1، 2009م.

[19] د. محمد أمين المداني، النظام الأوروبي لحماية حقوق الإنسان، مطبوعات مركز التوثيق والاعلام – وزارة حقوق الإنسان المغربية، يناير 2004م.

[20] د. محمد دروش فهيم، الجريمة وعصر العولمة: ملف لأشهر المحاكمات في مصر، النسر الذهبي للطباعة، مصر، 2000 م.

[21] د. محمد نور فرحات، المعايير الدولية وضمانات حماية حقوق الإنسان في الدستور والتشريعات المصرية، المواثيق الإقليمية لحقوق الإنسان، برنامج الأمم المتحدة الإنمائي، القاهرة 2006م.

[22] محمود إبراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإليكترونية، مكتبة الوفاء القانونية ط 1، الإسكندرية، 2014م.

[23] د. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمّان، 2009م.

[24] د. محمود شريف بسيوني " المحكمة الجنائية الدولية مدخل لدراسة أحكام وآليات الإنفاذ الوطني للنظام الأساسي" دار الشروق، الطبعة الأولى، 2004م.

[25] د. محمود شريف بسيوني، الوثائق الدولية المعنية بحقوق الإنسان، المجلد الثاني، دار الشروق، القاهرة، 2003م.

[26] د. ممدوح خليل بحر، حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009م.

[27] د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، النهضة العربية، ط 1، 2004م.

[28] هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، دار النهضة العربية، 2005م.

[29] د. هلالي عبد اللاه احمد، الجوانب الموضوعية والاجرائية لجرائم لمعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م)، دار النهضة العربية، القاهرة، 2006م.

[30] د. هلالي عبد اللاه احمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، النسر الذهبي، القاهرة، 2000م.

الرسائل :

[31] د. يونس عرب، جرائم الحاسوب، دراسة مقارنة، ماجستير، الجامعة الأردنية، 1994م.

[32] د. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراة، كلية الحقوق، جامعة عين شمس، 1997م

الدراسات:

[33] القاضي أنيس صالح جمعان، بحث بعنوان: التصنيف القانوني لجرائم الابتزاز الإلكتروني/ منصة اعرف حقك وقانونك: https://www.kurlye.com/

[34] د. سعاد قصعة، تحديات الأمن المعلوماتي في مواجهة الجريمة الإلكترونية في ظل الإعلام الجديد، مجلة المعيار مجلد: 24 عدد: 50، قسنطينة / الجزائر السنة: 2020م.

[35] المستشار/ د. صالح عبدالله المرفدي/ عضو المحكمة العليا للجمهورية، الجرائم المرتكبة على وسائل التواصل الاجتماعي: https://www.aden-tm.net/news/270205

[36] د. شمس عبدالله العمرو " قانون الأونسيترال النموذجي": a. https://alqalahnews.net/article/227724

[37] د. فادية أبو شهبة، الحق في الخصوصية – المجلة الجنائية القومية، مجلد 4 (مارس، يوليو، نوفمبر)، 1997م.

[38] فريد ناشف، آليات التعاون الدولي في مكافحة الجريمة الإلكترونية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 8، العدد 1، جامعة بليدة، الجزائر، 2013م.

[39] د. يونس عرب، دور حماية الخصوصية في تشجيع الاندماج بالمجتمع الرقمي، ورقة عمل /ندوة اخلاق المعلومات، نادي المعلومات العربي – 16-17 أكتوبر 2002عمان ، الأردن.

[40] تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، بانكوك، في الفترة 18-2005/4/25م، وثيقة رقم A/CONF.203/14

[41] مجلة الأمن العام، القاهرة، يناير 1985م، عدد (108).

[42] الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، مركز هردو لدعم التعبير الرقمي القاهرة 2014م : www.hrdoegypt.org / info@hrdoegypt.org

المواقع الإلكترونية:

[43] المؤتمر الدولي لأمن المعلومات الإلكترونية:

[44] http://www.albayan.ae/economy/1135159674-001-2005-12-22-1.128467

[45] المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت:

[46] http://news.wata.cc/news.php?action=vfc&id=748

[47] المؤتمر الدولي الثاني والثلاثون لمفوضي الخصوصية وحماية البيانات– القدس 2010م:

[48] http://www.justice.gov.il/PrivacyGenerations/Ar/privacy.htm

[49] موقع مفوضي الخصوصية وحماية البيانات (مونتريال 2007م / مكسيكو – 2011م):

[50] http://www.unep.fr/ozonaction/information/mmcfiles/7473-a-OASI2010_OutOfTheMaze.pdf

[51] الأمن السيبراني: المصدر / www.cisco.com

[52] منظمة التعاون والتنمية في الميدان الاقتصادي، المبادئ التوجيهية التي تحكم حماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية:

[53] https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

[54] موقع الأمم المتحدة : https://news.un.org/ar/story/2024/08/1133441

[55] موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة:

[56] https://www.unodc.org/e4j/ar/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html.

[57] قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع 1996:

[58] https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/ar/ml-ecomm-a_ebook.pdf.

القوانين اليمنية:

[59]قانون رقم (٢٥) لسنة ١٩٩٠ م بشأن الصحافة والمطبوعات.

[60]القانون رقم (38) لسنة 1991م للاتصالات السلكية واللاسلكية والمعدل بالقانون (33) 1996م.

[61]قانون رقم (64) لسنة 1991م بشأن البريد والتوفير البريدي.

[62]القانون رقم (٢١) لسنة ١٩٩٢م بشأن الإثبات (وتعديلاته).

[63]القانون رقم (12) لسنة 1994م بشأن الجرائم والعقوبات.

[64]القانون رقم (13) لسنة 1994م بشأن الإجراءات الجزائية.

[65]القانون رقم (40) لسنة 2006 بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية.

[66]القانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات.

[67]قانون مكافحة غسل الأموال وتمويل الإرهاب (1) 2010م وتعديلاته بالقانون (17) 2013م.

ـ المراجع الاجنبية :

[1] Recommendation of the council concerning guidelines fo the security of information's system، 26 November 1992.

[2] BAKKER "R" (computer security hand book) London second edition 1990.

[3] Daniel Kaplan، Informatique، libertées، identities، Fyp Edition،1er avril.2010.

[4] Malcom Anderson: " Policing the world: Interpol the Politics of International Police Co- Operation " ، Clarendon press.Oxford،1989.

[5] Westin، A F ، Privacy and Freedom، New York، Atheneum. (1967).

[6] Miller،(1971)،The Assault on Privacy،Ann Arbor، University of Michigan Press.

[7] MATTATIA Fabrique، Traitement des donnes personnelles- Le guide juridique- la loi informatique et libertés de la CNIL jurisprudences، Edition Eyrolles، Paris، 2013.

[8] Francesco Miani: le cadre réglementaire des traitements de données personnelles effectues au sein de l'union européenne، revue trimestrielle de droit européen، Dalloz،n2، 2000.