دور التشريعات والقوانين الوطنية والدولية الحاكمه لحماية امن المعلومات

د. نزيه محمد على*

مقدمة

رغم التطورات والمزايا العديدة التي أحدثتها الثورة التكنولوجية خاصة في مجال الاتصالات الامر الذي جعل العالم قرية صغيرة ونتج عن ذلك سهولة وسرعة في نقل المعلومات والبيانات والأخبار - رغم ذلك - ظهرت عيوب كثيرة لأستخدام وسائل الاتصال الحديثة التي تعتمد على احدث البرامج في مجال تكنولوجيا الاتصالات من هذه العيوب واهمها هو سهولة الحصول على البيانات والمعلومات الشخصية وعلى اي معلومة توضع على الحاسب الالى اواى جهاز ذكى مثل (التليفونات المحمولة) وأصبع الاطلاع على هذه المعلومات أمر سهل وبسيط بأستخدام برامج معينة لهذا الغرض والتى تسمى برامج (الهكر)

ولذلك ظهر فى الفكر القانونى المعاصر مصطلح الجريمة المعلوماتية إلى يكون محلها الاعتداء على بيانات ومعلومات خاصة وسرية لأحد الافراد او الهيئات.

وقد حاول الكثير من الفقه التصدى لتعريف هذه الظاهرة وحاول ايضا تعريف الجريمة المعلوماتية و من الفقهاء من عرف هذه الجريمة ، بأنها (سوء استخدام الحاسب الالي ويشمل حالات الولوج غير المصرح به لحاسب المجنى عليه لسرقة بياناته ومعلوماته الخاصة وقد يترتب على سرقة هذه المعلومات نتائج خطيرة من ذلك معرفه بيانات حسابات الشخص البنكية وكذلك معرفة الارقام السرية لبطاقات الأئتمان مما يؤدى الى سهولة سرقة حسابات الشخص وتحويلها للجانى.

مما سبق نجد أن سبب ارتكاب هذه الجرائم هي استخدام تكنولوجيا الاتصالات وبرامج الحاسب الآلى بوجه خاص . وهذا يضعنا فى موضع صعب في حاله محاولة أثبات هذه الجريمة في حالة ارتكابها عن طريق الانترنت ووسائل الاتصال الحديثة.

لكل ذلك اعتبر القانون الدولي هذه الجرائم جرائم ماسة بحقوق الانسان حيث انها تعتدى على حقه في السرية الحق الذي يعتبر من الحقوق اللصيقة بالشخصيه وهذا الامر الذي جعل القانون الدولي يتدخل لتجريم هذه الافعال فضلا على تجريم هذه الافعال في القوانين الداخليه للدول حيث اصدرت كثير من الدول قوانين خاصه لحماية البيانات الشخصية ، وكان اول قانون لحماية البيانات صدر في المانيا عام ١٩٧١

ولكن سوف نتعرض في بحثنا هذا للقواعد الدولية التي تهدف لحمايه امن المعلومات.

فعلى سبيل المثال وجدنا اتفاقية مجلس اوروبا الصادر في عام ١٩٨١ وكان موضوع هذه الاتفاقيه حمايه الافراد في ما يتعلق بالمعالجه الالية للبيانات الشخصية، هذا بالاضافه الى المبادئ التوجيهية بشأن معالجة البيانات الشخصيه الصادره عن الاتحاد الاوروبي.

ولأهمية البيانات والمعلومات السريه ولان الاعتداء عليها يعتبر اعتداء على حق من حقوق الانسان كما ذكرنا فقد اشارات الماده 12 من الاعلان العالمي لحقوق الانسان والماده 17 من العهد الدولي الخاص بالحقوق المدنيه والسياسيه تنصان على انه لا يجوز التدخل التعسفي في خصوصيات الفرد او اسرته او منزله او مراسلاته وان لكل شخص الحق في حمايه القانون من هذه التدخل .

من جماع ما سبق سوف نحاول إلقاء النظرعلى التشريعات والقوانين الحاكمه لحماية امن المعلومات باعتباره من حقوق الانسان الذي يجب على المجتمع الدولي حمايته فضلا صدور عده قوانين داخليه لكثير من الدول فى هذا المجال.

---

* دكتور فى الحقوق قسم القانون الدولى العام

The role of national and international legislation and laws governing the protection of information security

Introduction

Despite of many developments and advantages which has brought by the technological revolution, especially in the field of communications, which made the world a small village, this resulted in the ease and speed of transmitting information, data and news - despite this - many drawbacks appeared to use a modern means of communication that depend on the latest programs in the field of communication technology, from these disadvantages the most important of which is the ease of obtaining personal data and information and any information placed on a computer or any smart device such as: (mobile phones). And looking at this information became easy and simple by using specific programs for this purpose, which is called hacker programs. Therefore, in contemporary legal thought, the term "information crime" appeared in the place of attacking private and confidential data and information for an individual or organization.

Many jurisprudence has tried to address the definition of this phenomenon and also tried to define the information crime, and among the jurists who defined this crime as: (misuse of the computer and it includes cases of unauthorized access to the victim's computer to steal his data and private information. Theft of this information may have serious consequences for this includes knowing the person's bank account data, as well as knowing the secret numbers of credit cards, which leads to the ease of stealing the person's accounts and transferring them to the offender).

From the above, we find that the reason for committing these crimes is the use of communication technology and computer programs in particular. This puts us in a difficult position in the case of trying to prove this crime in the event that it was committed through the Internet and modern means of communication. For all this, international law considers these crimes as crimes against human rights, as they infringe on his right to confidentiality, a right that is closely related to his personality. Especially for the protection of personal data, the first data protection law was passed in Germany in 1971.

But we will expose in this research to the international rules which aim to protect the information security, for example, we found the convention of the Council of Europe issued in 1981 and the subject of this agreement was the protection of individuals regarding to the automated processing of personal

data, in addition to the guidelines on the processing of personal data issued by European Union.

Because of the importance of confidential data and information, and because an attack on it is considered an attack on a human right, as we mentioned, Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights stipulate that it is not permissible to arbitrarily interfere with the privacy of an individual, his family, home, or his correspondence. And that every person has the right to the protection of the law from such interference.

From all of the above, we will try to look at the legislation and laws governing the protection of information security as a human right that the international community must protect, in addition to the issuance of several internal laws for many countries in this field.

أولا: موضوع الدراسة

هو التشريعات والقوانين الحاكمة لامن المعلومات فنظرا للحاجة الماسة للمشتغل بالقانون فيما يتعلق بالإجرام المعلوماتي أو الاليكتروني ، ناهيك عن أن بوادر هذا الموضوع بدأت تظهر مع زيادة وتيرة النمو المتسارع الذى تشهده مصر في استخدام النظم المعلوماتية فضلا عن ظروف السياسة الدولية والتبعية التكنولوجية في قطاع المعلوماتية ادى ذلك الى وجود مناخ ملائم لانتهاك حرمة البيانات الشخصية وحق الإنسان في الخصوصية والمساس بالأمن القومى والسيادة الوطنية.

وهذا البحث محاولة لإلقاء الضوء على تنوع وتعدد المخاطر التي تتعرض لها المعلومات ، وكذلك توضيح المحاولات التي تقوم بها الدولة للحد من تلك المخاطر عن طريق سن القوانين والتشريعات التى من شأنها تحقق حماية لامن المعلومات .

ثانيا :اهمية الموضوع

أصبح حماية المعلومات في عصر العولمة أمراً بالغ الأهمية من أجل ضمان استمرارية الأعمال، حيث إن التصدي للتهديدات الأمنية لنظم المعلومات أصبح تحديا يواجه العديد من الدول، فأمن المعلومات لا يعني تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها فقط ولكن مكافحة الجريمة المعلوماتية ومنعها من الظهور .

واعترافا بذلك بذلت الدولة جهوداً كبيرة في إدارة ومعالجة أمن المعلومات، وأصبح من الضروري عليها أن تهتم بوضع نظم وإجراءات تعمل على الحد من تلك المخاطر ، ووضع نظام جيد لإدارتها والعمل على نجاح برنامجها الأمني .

ومن هنا تأتي أهمية البحث في كون محاولة متواضعة في تسليط الضوء على الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها وكيفية الحماية التي وفرها المشروع في قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

ثالثا أهداف الدراسة:

1-اعطاء فكره اوضح واعمق عن موضوع اليات حماية امن المعلومات وطرق تطبيقه واهدافه وعناصره

2-تسليط الضوء على الحماية القانونية لامن المعلومات والخصوصية المعلوماتية .

3- الكشف عن مخاطر التقنيات الحديثة على الحق في الخصوصية المعلوماتية.

4- إيضاح الحماية التي وفرها المشروع فى قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020

رابعا: مشكلة الدراسة:

إنّ التقدم التكنولوجي الكبير، وتطوّر وسائل التواصل والاتصال المتنوعة، وانفتاح العالم على بعضه، واعتماده على إرسال شتى أنواع البيانات خلال الشبكات، كلّ ذلك أدى إلى إحداث خطر على تسرّب هذه البيانات، ووصولها للأشخاص الخاطئين، أو المنافسين، وبالتّالي أصبحت الحاجة الملحّة للحفاظ على أمن المعلومات .

فالمشكلات الأمنية التي أوجدتها شبكات الحاسب وبخاصة شبكة الانترنت والتي تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، بالإضافة إلى أن شبكة الانترنت صارت وسيلة اتصال فعالة للعصابات والمجرمين والمخالفين للقانون والأعراف الاجتماعية والأخلاقية السائدة، وتوفر بيئة خصبة لترويج التجارة المحرمة وغسيل الأموال والجرائم المنظمة، وتشكل ميداناً حديثاً من ميادين الحرب الإلكترونية. كما أنها تؤمن تربة مناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية .

لذلك كان من الضرورى القاء الضوء على الجرائم المعلوماتيه والطرق القانونية لمكافحتها و تسليط الضوء على مشكلة الإجرام في القطاع المعلوماتي، وطبيعة التهديدات التى يتعرض لها نظم المعلومات والطرق المتبعة لماجهتها

خامسا : منهج الدراسة :

سنتناول موضوع الدراسة من خلال المنهج الوصفى باعتباره المنهج الأكثر انسجاماً مع طبيعة وأهداف هذا البحث من خلال جمع الحقائق والبيانات عن ظاهرة الاجرام المعلوماتى، مع محاولة تفسير هذه الحقائق تفسيرا كافيًا، بالإضافة إلى المنهج التحليلي لدارسة المواد القانونية الخاصة بحماية امن المعلومات وصولا إلى انجع الحلول للقضاء على الجرائم المعلوماتية في إطار تنظيم قانوني متكامل يتلاءم مع متطلبات العصر.

ونعرض لأوجه القصور التي شابتها، وطرق معالجتها من خلال طرح عدد من التوصيات الهامة.

سادسا :خطة الدراسة:

المبحث الاول : الجرائم المعلوماتية

المطلب الاول : ماهيه الجرائم المعلوماتيه

المطلب الثانى : الأدلة في الجريمة المعلوماتية

المبحث الاول

الجرائم المعلوماتية

المطلب الاول

ماهيه الجرائم المعلوماتيه

لقد مرت الجريمة المعلوماتيه او الالكترونية نتيجة للتدرج في الظاهرة الاجرامية الناشئة عن بيئة الحاسب الآلي بعده اصطلاحات ابتداء من إساءة استعمال الحاسوب مروراً باصطلاح احتيال الحاسوب ثم اصطلاح الجريمة المعلوماتية فإصطلاح جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر ثم جرائم التقنية العالية وجرائم الهاكرز وأخيرا جرائم الانترنت([1]).

هذا ولا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية إذ منهم المضيق لهذا المفهوم ومنهم الموسع ومنهم من يقسم تعريف الجريمة الإلكترونية الى ثلاث اتجاهات([2]).

فمن التعريفات المضيقة للجريمة المعلوماتية أنها :

1- " الفعل غير المشروع الذي يتورط في إرتكاب جرائم الحاسب الآلي"

2- إنها " الفعل الإجرامي : الذي يستخدم في إقترافه الحاسب الآلي كأداة رئيسية"

3- أنها " مختلف صور السلوك الإجرامي التي ترتكب بإستخدام المعالجة الآلية للبيانات

ومن التعريفات الموسعة لمفهوم الجريمة المعلوماتية([3])

تعريف الفقيهان (ميشل- ورود) حيث يعرف الجريمة المعلوماتية بأنها سوء إستخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحساب المجني عليه أو بياناته .

كما تمتد جريمة الحاسب لتشمل الإعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به ، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان وإنتهاك ماكينات الحساب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو أي مكون من مكوناته.

اذن تعريف الجريمة الإلكترونية له ثلاث اتجاهات وذلك على النحو التالي:

الاتجاه الاول:يستند أصحاب هذا الرأي إلى لزوم أن يكون نظام الحاسب الآلي هو محل الجريمة، فيجب أن يتم الاعتداء على الحاسب الآلي أو على نظامه، فقد عرفها انصار هذا الاتجاه بقوله: هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه([4]).

الاتجاه الثاني: ويستند أنصار هذا الاتجاه إلى معيار شخصي يستوجب أن يكون فاعل هذه الجرائم ملما بتقنية المعلومات واستخدام الحاسوب لإمكانية اعتبارها من جرائم الحاسب الآلي. **وعليه تعرف الجريمه المعلوماتيه بأنها([5]):** أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا، وبناء على ذلك لا بد أن يكون مرتكب الجريمة الإلكترونية على درجة كبيرة من المعرفة التكنولوجية بالحاسبات لتلاحقه هذه الجريمة قانونيا كما ان هذا التعريف أخذت به وزارة العدل الأمريكية في تقريرها الصادر سنة 1989.

الاتجاه الثالث: يستند إلى وسيلة ارتكاب الجريمة فيشترطون وجوب ارتكابها بواسطة الحاسب الآلي، كما عرفها انصار هذا الاتجاه بأنها: كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب، أو هي كل جريمة تتم في محيط الحاسبات الآلية ، وبالتالي يعد هذا التعريف توسعا كبيرا في مفهوم الجريمة الإلكترونية كونه يعد الجريمة التي تقع على سرقة الحاسوب وما يتعلق به جريمة إلكترونية([6]).

واخيرا فان هناك تعريفات اخرى منها التعريف الذى اقترحته مجموعة من خبراء منظمة التعاون الاقتصادى والتنمية في اجتماع عقد بباريس في عام 1983 وذلك لبحث الجريمة المرتبطة بالمعلوماتية وورد فيه أنه" كل سلوك غير مشروع أو غير أخلاقى أو غير مصرح به يتعلق بالمعالجة الآليه للبيانات أو بنقلها" لكنه تعريف فيه من المرونه والاتساع ما ادى على

التسوية بين السلوك غير المشروع قانوناً والسلوك الذى لا يرتب سوى استهجانه اخلاقيا ذلك أنه لا تلازم دائما ما بين الفعل المستهجن اخلاقيا وذلك المؤثم قانوناً([7]).

وعرفت الجريمة المعلوماتية كذلك بأنها نشاط جنائى يمثل اعتداءً على برامج وبيانات الحاسب الآليكترونى([8]).

والجدير بالذكر ان المشرع المصري لم ينص على تعريف محدد لجرائم تقنية المعلومات وهذا اتجاه صائب ومحمود، حيث أن الرأي الغالب والمتفق عليه لدي جانب عريض من فقهاء القانون أن المشرع ليس مختصاً بوضع تعريف للجريمة، فذلك العمل يدخل في صميم اختصاص ومهام رجال الفقه والقضاء، نظراً لتطور الجريمة وتنوع أساليب ارتكابها وتعدد صفاتها خاصة جرائم الانترنت([9]) وتقنية المعلومات، وإنما يمكن وضع أسس عامة أو أركان للجريمة من خلالها يمكن التعرف عليها أو تحديد السلوك الإجرامي المستحدث المكون للجريمة، فإذا ما توافر هذا السلوك أو العناصر أو الأركان أصبح الفعل أو العمل المرتكب عملاً إجرامياً يستوجب العقاب، على أن تترك مهمة البحث في مدي توافر تلك العناصر أو الأسس أو الصفات السلوكية لاجتهاد قاضي الموضوع.

من خلال ما سبق يمكن أن نعرف الجريمة المعلوماتية بأنها كل فعل أو امتناع مُجرم وغير مشروع يعاقب عليه القانون، يتم بواسطة شخص يتمتع بقدر من الذكاء الفني والتقنية العالية، ويقوم على مجموعة من العناصر بشكل مباشر أو غير مباشر والمتصلة اتصالاً وثيقاً بالحاسب الآلي ووسائل التقنية الحديثة والتي لا يمكن ان تنشأ وجودها من الأساس دون تحقق هذا الارتباط التقني بالحاسب الآلي([10])

المطلب الثانى

الأدلة في الجريمة المعلوماتية

هذه الجريمة كغيرها من الجرائم لها أركانها وعناصرها وتمر بذات المراحل التي تمر بها الجريمه كما في شأن الجرائم العادية كالسرقة والقتل وهذه المراحل هى التفكير في الجريمة والتحضير لها ثم تنفيذ الجريمة ومحاولة التخلص من آثارها.

ولذلك تثور هنا مسالة استخلاص الدليل الذي تثبت به الجريمة المعلوماتية([11])، وإذا كان الاعتراف هو سيد الأدلة يليه شهادة الشهود فضلاً عن القرائن والآثار الناجمة عن النشاط الإجرامي بما لها من دور في إثبات الجريمة وكشف الحقائق فيها بالنسبة لجرائم قانون العقوبات فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية مما حدا البعض الى القول بأن قواعد قانون العقوبات تواجه تحديات إزاء مواجهة الجريمة المعلوماتية وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح إجتماعية واقتصادية ارتبطت بظهور وانتشار جهاز الحاسب الآلى وشبكة المعلومات الدولية(الانترنت), مما أدى الى ظهور طائفة جديدة من الادله خاصه بالجريمه المعلوماتيه اطلق عليها الادله التقنيه كالدليل الرقمي([12]).

ولقد كان ظهور الجريمة المعلوماتية عاملاً حاسماً في قيام كثير من الدول بسن تشريعات جديدة أو تعديل تشريعاتها القائمة لمواجهة الجريمة المعلوماتية ومن بينها المشرع المصرى الذي تدخل جدياً لمواجهة هذا النوع من الجرائم .([13])

وفي 18 أغسطس عام 2018 صدَّق الرئيس السيسي على قانون جرائم تقنية المعلومات، وفي 27 أغسطس من نفس العام تم التصديق على قانون تنظيم وسائل الإعلام، والتي أدت إلى تقنين مراقبة الحياة الإلكترونية وبالتالي تقييد الحريات الرقمية، وبصدور قانون حماية البيانات الشخصية والتصديق عليه في يوليو عام 2020 تسعى الحكومة المصرية بخطًى متسارعة إلى فرض سيطرتها على المجال الرقمي وتداول البيانات، وهو الأمر الذي ينبغي أن يتم وفقًا للمعايير الدولية والحقوق الأساسية المنصوص عليها ضمن الدستور وبقية التشريعات المصرية، وذلك للحفاظ على حق الأفراد في التعبير، وكذلك ضمانًا للحقوق والحريات الشخصية، وحتى لا يتم استخدام تلك البيانات بشكل غير قانوني من قِبل السلطات المصرية.

وحيث ان موضوع إثبات الجريمة المعلوماتية من الموضوعات التي تتميز بندرة التطبيق القضائي فانه تبرز للوجود مسألة صعوبة جمع الاستدلالات والأدلة في الجريمة المعلوماتية إذ أن هذه النوعية من الجرائم توجد في بيئة لا تعتمد التعاملات فيها- أصلا- على الوثائق والمستندات المكتوبة بل على نبضات إليكترونية غير مرئية لا يمكن قراءتها بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل ويمكن في أقل من الثانية العبث بها أو محوها بالكامل لذلك فإن المصادفه وسوء الحظ لهما دور كبير في اكتشافها وذلك أكثر من الدور الذى تلعبه أساليب التدقيق والرقابة([14]).

و لعل من أهم المواضيع حساسية موضوع الدليل([15]) الذي تثبت به الجريمة المعلوماتية أو الجريمة المتعلقة بالحاسب الآلى([16])، حيث يواجهه قانون العقوبات تحديات إزاء مواجهة الجريمة المعلوماتية وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح اجتماعية واقتصادية ارتبطت بظهور وانتشار جهاز الحاسب الآلى وشبكة المعلومات العنكبوتية (الانترنت)([17])

لذلك وبعد أن أصبح المجتمع المعلوماتى حقيقة واقعة حيث تعتمد المجتمعات المعاصرة في تسيير شئونها على تقنيات الحاسبات والمعلومات ومن ثم يتعين على أجهزة العدالة الجنائية مع تقلص الدور التقليدي للوثائق في الإثبات وازدياد مطرد في كم المعلومات المنتجة أو المعروضة في أوعية- لا ورقية مستحدثة- أن تتعامل في ممارستها لحق المجتمع في الدفاع عن كيانه ضد الإجرام مع أشكال مستحدثة من الأدلة غير المادية وذلك في مجال الإثبات الجنائى وهو ما يفرض على الفكر القانوني من جهة أن يسعى دوماً لتطوير أساليب كشف الجريمة المعلوماتية والوسائل المستخدمة في عمليات البحث الجنائي والتحقيق وهو ما يتطلب برامج تخصصية في التدريب لاكتساب هذه المهارات في أعمال الإستدلال والتحقيق المعلوماتى ومن ناحية أخرى يجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم المعلوماتية- وتحديثها على نحو يكفل إستجابتها بشكل كاف وبدون أن تتعرض حقوق الأفراد وحرياتهم للخطر عند الإثبات([18]).

لعل المبررات السابقة في شأن صعوبة استخلاص دليل الإثبات ([19])تحث بالتأكيد على ضرورة مسارعة رجال الاستدلال والتحقيق بتطوير وسائلهم البحثية وقدراتهم العلمية وليس بالضرورة أن يكون المحقق خبيراً في الحاسب الآلى ولكن لابد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلى وحسن استغلالهم في كشف الجرائم وجمع الأدلة كما انه من الضرورى أن يكون المحقق ملماً بالإجراءات الإحتياطية التي ينبغى اتخاذها نحو مسرح الجريمة في الجريمة المعلوماتية والتدابير اللازمة لتأمين الأدلة و القول ذاته بالنسبه للقضاة من حيث ضرورة تسليح القاضي الجنائي بتقنية وعلوم الحاسب الآلي لمواكبة المناقشة العلمية للمخرجات الالكترونية([20]) .

المطلب الثالث

أهم صور الإستخدام غير المشروع للحاسب الآلي([21])

أن الجرائم المرتبطة بالاستخدام غير المشروع للحاسب الآلى كثيرة ومتنوعة فهى تشمل الاحتيال المعلوماتى والقرصنه(برامج النسخ غير المشروع) والتجسس المعلوماتى في نطاق قطاع الأعمال والتخريب المعلوماتى والإرهاب وانتهاك حرمه الحياة الخاصة.

فالمشرع الفرنسي على سبيل المثال اهتم اهتماماً بالغاً بالمعلومات المخزنة عن طريق شبكة الانترنت ,بصفة خاصة إذا كانت لها الصفة الرسمية أو الحكومية ,فجرم عمليات الدخول أو البقاء غير المشروع على المواقع أو البريد الالكتروني لأية جهة حكومية ,كما جرم عمليات إتلاف المعلومات المخزنة عبر الحاسب أو عبر شبكة الإنترنت ,وذلك بقانون يناير 1988 بشأن جرائم الغش والاحتيال المعلوماتي ,لكن الملاحظ أن المشرع الفرنسي ينضم إلى الجانب الذي يرجح أن تكون النصوص العقابية ضمن قانون العقوبات الفرنسي.

وفي الولايات المتحدة الأمريكية أخذ المشرع الأمريكي بالعديد من الضمانات لحماية أمن المعلومات بصفة عامة, وعلى الأخص حماية المعلومات الرسمية والوثائق الحكومية ,فصدر قانون إساءة استخدام الحاسوب عام , 1984 ثم قانون امن الحاسوب لسنة , 1987 والذي أتاح للوكالات الفيدرالية اتخاذ الخطوات الملائمة لتأمين وحماية أنظمة حواسبها ,ثم توالت التشريعات ذات الصلة بتنظيم الاستخدام الآمن للحاسب الآلي ,والتي ضمنت توفير الحماية القانونية للوثائق والمستندات الحكومية وأنظمة المعلومات التي تعتمدها المؤسسات الرسمية في عملها ,واعتبرها القانون من المعلومات المتعلقة بالأمن القومي وقد كانت المادة 1030 من قانون العقوبات الفيدرالي تحمي الخصوصية الفردية ,من خلال تجريم الوصول غير المشروع أو غير المصرح به إلى المعلومات والسجلات المصرفية المتعلقة بالعملاء مع المؤسسات المالية, ثم وسع الكونجرس من نطاق تطبيق الحماية عام , 1996 لتشمل أيضاً المعلومات المخزنة على أجهزة الحاسب الحكومية ,وكذلك أجهزة الحاسب المستخدمة في الاتصالات بين الولايات والاتصالات الخارجية.

وبشكل عام يمكن أن تصنف جرائم الحاسب الآلي إلى صنفين:

الجرائم ذات الجانب الاقتصادي:

وذلك كالاحتيال المعلوماتي والتجسس في نطاق قطاع الأعمال بهدف توظيف هذه المعلومات والبيانات ضد المجني عليه، وقرصنة برامج الحاسب الآلي، وإتلاف المعلومات سواء كان للبيانات نفسها أم الوسائط التي تحمل هذه البيانات. وسرقة الخدمات أو الاستعمال غير المصرح به لنظام الحاسب الآلي.

الجرائم المتصلة بانتهاك حرمة الحياة الخاصة:([22])

وذلك باللجوء إلى أساليب غير مشروعة للحصول على بيانات صحيحة عن الأفراد بطريق غير مشروع، أو إفشاء بيانات شخصية للغير بطريقة غير مشروعة، وهي التي تمس الأمور الجوهرية في حياة الأفراد، ، والغاية من حماية هذا الحق ضمان السلام والسكينة لهذا الجانب من الحياة غير المتصل بالأنشطة العامة بجعله بمنأى عن التقصي والإفشاء للغير.

المبحث الثانى

الجرائم المعلوماتية والعقوبات المقررة لها

قدمت وسائل التقنية الحديثة مزايا ومساعدات عديدة للإنسانية لمواجهة التطورات والاحتياجات الحياتية، خلفت أيضاً العديد من المساوئ والسلبيات الضارة، حيث استخدمها المجرمون في تحقيق أهدافهم غير المشروعة فكانت أداة جديدة غيرت من شكل الجريمة بصفة عامة سواء كانت أداة لارتكابها ، أو مسرحاً لها، وهو ما أطلق عليه –الإجرام الحديث([23]) الذي أفرز نوعية جديدة من الجرائم سميت ،(الإجرام التقني) بجرائم التقنية، أو جرائم المعلوماتية ارتباطاً بشبكة المعلومات الدولية)([24])

والجدير بالذكر أن المشرع المصري تناول تحديد هذه النوعية من الجرائم في الباب الثالث من قانون مكافحة جرائم تقنية المعلومات، وأفرد لكل منها عقوبة خاصة بها تتناسب وجسامة الجرم المرتكب ومدي خطورته وإضراره بالأفراد والمجتمع، أي تحديد العقوبات الكفيلة بمكافحة هذه النوعية من الجرائم المستحدثة ومعاقبة مرتكبيها، وتتأرجح هذه العقوبات ما بين التخفيف والتشديد حسب الخطورة الإجرامية وحجم الأضرار المترتبة عليها، هذا وقد نص المشرع على ضرورة الأخذ في الاعتبار عند تطبيق هذه العقوبات عدم الإخلال بأي عقوبة أشد منصوص عليها في قانون العقوبات أو أي قانون آخر.([25])

المطلب الأول

جرائم الشبكات وأنظمة وتقنيات المعلومات

أولاً :جريمة الانتفاع بدون حق بخدمات الاتصالات والمعلومات وتقنيتها:

يقصد بالانتفاع هو تحقيق قدر معين من الاستفادة سواء أكانت استفادة مادية أو معنوية أو أدبية، وقد اعتبر المشرع المصري أن هذا الانتفاع أو الاستغلال واستخدام هذه التقنية دون

حق مشروع من قبيل الأفعال غير المشروعة المجرمة أو القرصنة التي تستوجب العقاب، بل اعتبرها جريمة تشبه إلى حد كبير جريمة السرقة، وعرفها في المادة ١٣ من قانون مكافحة تقنية المعلومات بأنها كل انتفاع يتم بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات بخدمة اتصالات أو خدمة من خدمات قنوات البث المسموع أو المرئي)([26])

وقد نهج المشرع الإماراتي([27]) ذات نهج المشرع المصري بتجريم فعل الانتفاع دون وجه حق في المادة ٣٤ من قانون المكافحة التقنية الإماراتي، ولكنه لم يقصرها على مجرد الانتفاع الفردي فقط، بل أضاف إليها فعل تجريمي أخر وهو تسهيل الانتفاع للغير، وأفرد لها بذات المادة عقوبة أكثر تشدداً عما أورده المشرع المصري .

أما على الجانبين الكويتي والسعودي فلم يرد بهما أية نصوص تتطرق لمثل هذا الاتجاه التجريمي، كما لم يرد مثل هذا النص بنصوص الاتفاقية العربية لمكافحة الجريمة التقنية.

ثانياً :جريمة الدخول غير المشروع

يقصد بالدخول غير المشروع أو الهكترة هو النفاذ المتعمد غير المشروع لأجهزة وأنظمة الحاسب الآلي أو لنظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني من خلال اختراق وسائل وإجراءات الحماية لها بشكل جزئي أو كلي لأي غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح أو هو دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع اليكتروني أو نظام .معلوماتي، أو شبكة حاسبات آلية وغير مصرح لذلك الشخص بالدخول إليها) ولم يرد بقانون تقنية المعلومات المصري تعريف واضح ومحدد لفعل الدخول غير المشروع إلا أنه من الجائز استنباط هذا التعريف من نص المادة (١٤)منه بأنه كل دخول يحدث عمدا، أو بخطأ غير عمدي والبقاء بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه."

وقد عاقب المشرع المصري على مجرد ارتكاب فعل الدخول غير المشروع إلى مواقع أو حسابات خاصة أو أنظمة تقنية المعلومات والبقاء بها دون وجه حق، سواء أكان هذا الدخول قد تم بعمد أو بدون عمد عن طريق الخطأ، وبشرط أن يكون هذا الدخول محظوراً([28])، أما وإن تسبب هذا الدخول غير المشروع في حدوث أضرار معلوماتية أو نتج عنه مخاطر تتمثل في إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، فهنا الوضع يختلف تماماً، حيث شدد المشرع المصري وضاعف من حد العقوبة المقررة له)

ويكمن الهدف من وراء هذا التجريم في حماية الأنظمة والبرامج المعلوماتية من عمليات التطفل والقرصنة عن طريق ما يعرف بالدخول غير المشروع سواء أكان الدخول في جزء من النظام أو في جميع أجزاءه أو في كافة الأنظمة التقنية([29]).

وقد سلك المشرع الكويتي في المادة الثانية من قانون مكافحة جرائم تقنية المعلومات ذات مسلك المشرع المصري بتجريم ذات الأفعال، وضاعف من حد العقوبة المقررة لهذه الأفعال

إذا ما اقترنت جريمة الدخول غير المشروع بحالات أخري تستوجب التشديد نظراً لخطورتها وجاء ذلك في المادتين الثانية والثالثة من ذات التقنيين.

كما ذهب المشرع الإماراتي إلي تجريم فعل الدخول غير المشروع إلى موقع أو نظام أو شبكة معلوماتية أو أية وسيلة تقنية معلومات، طالما تم ذلك دون تصريح أو تجاوز المصرح له حدود هذا التصريح، ولم يقف الأمر عند ذلك الحد فقط بل توسع المشرع الإماراتي وأدرج ضمن هذه الأفعال فعل البقاء في هذه الأنظمة أو الشبكات بصورة غير مشروعة حتى وإن كان الدخول الأول قد تم بطريقة مشروعة.

والجدير بالذكر أن المشرع الإماراتي كان حريصاً على متابعة كل تطور ووضع بين نصب عينيه ما اتبعه المشرع الكويتي وسار على خطاه في تشديد العقوبة المقضي بها إذا ما اقترن فعل الدخول بأفعال أخري تزيد من خطورة الفعل المرتكب من المادة الثالثة ، وهو ذات ما تبناه المشرع السعودي في الفقرتين خاصة وأنه قد حرص على مضاعفة حد العقوبة المقررة إذا كان فعل الدخول غير المشروع مقروناً بأي من الأفعال الضارة الآتية([30]):

١ - الوصول -دون مسوغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات

٢ - إذا كان الدخول بهدف إلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها

٣ - إذا كان الدخول غير المشروع إلى موقع إلكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني .

وفي جميع الأحوال نص المشرع السعودي على ضرورة أن لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية :

-ارتكاب الجاني الجريمة من خلال عصابة منظمة.

-شغل الجاني لوظيفة عامة، واتصلت الجريمة بهذه الوظيفة، أو كان ارتكابه للجريمة من خلال استغلاله لسلطاته أو نفوذه الوظيفية.

-التغرير بالقُصر ومن في حكمهم، واستغلالهم.

-إذا كانت هناك أحكام محلية أو أجنبية سابقة بالإدانة صدرت بحق الجاني في جرائم مماثلة.

ثالثاً :جريمة تجاوز حدود الحق في الدخول:

يقصد بها قيام أحد الأشخاص بالدخول إلى موقع أو حساب خاص أو نظام معلوماتي مستخدماً حقاً مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول، وقد جاء النص علي هذه الجريمة في المادة ١٥ من قانون مكافحة جرائم التقنية المصري، هذا وقد أفرد لها المشرع عقوبة مستقلة أخف وطأة عن سابقتها([31]).

وبذلك فقد جعل المشرع المصري من حق الدخول المشروع المقرون بأفعال التجاوز جريمة مستقلة يعاقب فاعلها بعقوبة أخف وطأة عن سابقتها التي ترتكب حال الدخول غير المشروع، وهو مسلك لم يرد في تشريعات الدول المقارنة التي تناولتها ضمن

جريمة الدخول غير المشروع ولم تتطرق أيا منها استقلالاً إلى حالة البقاء عقب انتهاء حالة الدخول المشروع، ونري من وجهة نظرنا أن هذه الجريمة هي تزايد غير مبرر، وكان يجب أن تدرج ضمن الجريمة سالفة البيان، وتأخذ ذات عقوبتها حتى وإن كانت ترتبط بحق مشروع مخول للجاني وهو حق الدخول المشروع

رابعا :جريمة الاعتداء على تصميم موقع:

تعد هذه الجريمة من أحدث الجرائم التي رصدتها بعض التشريعات الحديثة، وقننت لها نصوصاً عقابية وتجريميه مستقلة، وكان من بين هذه التشريعات بل وأهمها التشريع المصري الذي تناول هذه الجريمة في المادة 19 منه، وأسهب في ذكر الأفعال التي تعتبر انتهاك أو اعتداء على تصاميم موقع خاص بغير وجه حق .

هذا وقد حرص كل من المشرع الكويتي، والسعودي والإماراتي على إتباع ذات النهج بتجريم كل فعل ينطوي على اعتراض غير المشروع ومتعمد للبيانات والمعلومات المتداولة بوسائل التقنية المعلوماتية، أو الاعتراض غير المشروع والمتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

هذا وقد ضاعف كل من التشريع الكويتي والإماراتي، من حد العقوبة في حالة إذا ما أفشى الشخص ما تحصل عليه من معلومات عن طريق هذا الاعتراض.

وقد سار كل من التشريعين الكويتي، والسعودي على ذات نهج المصري بتجريم هذه الأفعال والسلوكيات المتعلقة بالاعتداء على تصاميم موقع سواء أكان مملوكاً ملكية خاصة لشخص طبيعي أو شركة أو مؤسسة أو منشأة.

أما بالنسبة للتشريع الإماراتي فلم يختلف الأمر كثيراً عن تشريعات سابقيه، حيث تناولت المادة الخامسة منه التأكيد على معاقبة كل من دخل بغير تصريح موقعاً إلكترونياً بقصد تغيير تصاميمه أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه، إلا أنه يؤخذ عليه تناوله تجريم هذه الأفعال والسلوكيات دون تحديد مدة عقوبة الحبس المقررة على مرتكبي هذه الجريمة على غرار ما فعلته التشريعات المقارنة التي تناولت تحديد مدة الحبس والغرامة بحديهما الأدنى والأقصى([32]).

وفي جميع الأحوال يؤخذ على كافة هذه التشريعات قيامها على النحو المتقدم بتناول هذه الجريمة بشكل مستقل في نصوص خاصة تتعلق بها في حين أن طبيعة هذه الجريمة تتشابه إلى حد كبير مع جريمة الاعتداء على سلامة البيانات والمعلومات والنظم المعلوماتية، ولا تخرج عن نطاقها، فكان من المتعين إدراجها ضمن هذه جريمة دون الحاجة لأن تدرج في نصوص خاصة بها.

خامسا :جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة:

لم يضع المشرع تعريفاً محدداً لهذه الجريمة، وإنما اكتفي بأن أشار في المادة ٢٠ من قانون تقنية المعلومات المصري إلى بيان صور وأساليب ارتكابها، والتي يمكن من خلالها وضع تعريف لهذه الجريمة بأنها كل فعل يصدر من أحد الأشخاص ويمثل انتهاك لخصوصية موقع أو بريد إلكتروني أو حساب خاص أو نظام معلوماتي يدار بمعرفه الدولة أو لحسابها أو لحساب أحد الأشخاص الاعتبارية العامة، أو مملوكاً لها، أو يخصها، سواء أخذ شكل الاعتداء، أو الاختراق، أو الدخول إليها، وسواء كان هذا الدخول متعمداً، أو بخطأ غير عمدي وبقى به بدون وجه حق، أو تجاوز حدود هذا الحق من حيث الزمان أو مستوى الدخول([33]).

وقد تشدد المشرع المصري في الفقرة الثانية من ذات المادة وضاعف من حد العقوبة في حالة إذا ما كان هذا الدخول قد تم بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، وجاءت الفقرة الثالثة من ذات المادة أكثر تشدداً في حالة إذا ما ترتب علي هذه الأفعال إتلاف للبيانات أو المعلومات أو الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكتروني، أو تدميرها أو تشويهها أو تغييرها أو تغيير تصاميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها، أو إلغائها كليا أو جزئيا، بأي وسيلة .

ولم نجد لمثل هذا النمط أو الشكل الإجرامي صدي بالنصوص والتشريعات المقارنة، حيث لم تتناول النص صراحة على تجريم مثل هذا النوع من الاعتداء التي تقع على البيانات والأنظمة المملوكة للدولة، بل تناولت فقط تجريم فعل الدخول غير المشروع وما يترتب عليه من تعديات بشكل عام دون التطرق إلى كون هذه الاعتداءات أو الانتهاكات تنصب على نظام معلوماتي خاص بالأشخاص أم بنظام حكومي خاص بالدولة، وقد اكتفي البعض منها بالإشارة إلى مجرد تشديد العقوبة إذا ما كان الاعتداء قد وقع على نظام حكومي أو بيانات ومعلومات حكومية([34]).

ومن بين هذه التشريعات التشريع الإماراتي الذي أشار إلى مجرد تشديد العقوبة حال ما وقع الاعتداء على نظام أو بيانات أو معلومات حكومية، ولم يأتي هذا التشريع بأي جديد بخصوص هذه الجريمة، ولم يتناول النص عليها بشكل مباشر وصريح مثلما فعل المشرع المصري، إنما يفهم اتجاه المشرع الإماراتي من قانون التقنية : نحو تجريم هذه الأفعال من خلال ما ورد في المواد من المعلوماتية الإماراتي والتي تتعلق بجرائم الدخول غير المشروع التي تناولت التجريم بشكل عام دون تحديد ما إذا كانت أفعال الاعتداء أو الانتهاك المجرم وقعت على أنظمة مملوكة ملكية شخصية أم مملوكة للدولة أو الحكومة.

واكتفي في البند رقم (٣) من المادة الثانية منه بتشديد حد العقوبة المقررة لهذه)الأفعال في حالة ما إذا انصب الاعتداد على بيانات أو معلومات شخصية ، عكس ما هو متبع لدي المشرع المصري في شأن هذه الجريمة، كما أشار في المادة الثالثة من ذات القانون إلى ضرورة تشديد العقوبة أيضاً في حالة أخري، وهى حالة ما إذا وقعت الجريمة من موظف أثناء تأدية وظيفته أو بسببها وتعتبر المادة الرابعة من التشريع الإماراتي من أكثر النصوص دلالة وتوافقاً مع ما نص عليه المشرع المصري من تجريم هذه الأفعال، المتمثلة في فعل الدخول بدون تصريح إلى أي موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلوماتية، أو وسيلة تقنية

معلومات، سواء كان الدخول، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية([35]) .

وضاعف المشرع من حد العقوبة في حالة إذا ما تعرضت هذه البيانات أو المعلومات للإلغاء أو الحذف أو الإتلاف أو التدمير أو الإفشاء أو التغيير أو النسخ أو النشر أو إعادة النشر وقد سايره في هذا الاتجاه المشرع الكويتي حيث لم يتناول أيضاً النص صراحة على هذه الجريمة أو الإشارة لفعل التجريم بشكل مباشر، وإنما أورد بعض الإشارات في نصوص متفرقة يفهم منها حظر هذه الأفعال دون النص على ما إذا كانت البيانات حكومية أو غير حكومية، وفي المادة الثالثة أشار إلى تشديد العقوبة في حال ما إذا كانت البيانات محل الاعتداء حكومية أو متعلقة بحسابات العملاء في المنشآت المصرفيه ولم يذهب المشرع السعودي بعيداً عن ذلك، فقد تناول في الفقرتين الثانية والثالثة من المادة الخامسة النص على ذات الأفعال الوارد ذكرها بالتقنين المصري وزاد عليها واعتبرها من قبيل الأفعال الإجرامية الخطرة واجبة العقاب([36]).

وقد سايرهم في ذلك المشرع الكويتي في المادة الرابعة منه ، ولكنه كان غير موفق في الصياغة القانونية، حيث يؤخذ عليه في هذه المادة إغفال وعدم ذكر بعض الأفعال والسلوكيات التي تؤدي إلى وقوع الجريمة مثل فعل التشويش أو محاولة الحد من كفاءة عملها أو إعاقتها أو اعتراض عملها أو قيام الجاني بإجراء معالجة إلكترونية للبيانات الخاصة بالشبكة المعلوماتية بدون وجه حق أسوة بما فعله المشرع المصري على النحو المتقدم .وبالنسبة لموقف المشرع الإماراتي أيضاً فلم يختلف كثيراً عما ذهب إليه المشرع الكويتي من عدم التوسع في ذكر الأفعال والانتهاكات التي تمثل اعتداء على سلامة الشبكة المعلوماتية وأغفل أيضاً ذكر البعض منها

سادسا :جريمة الاعتداء على سلامة شبكة المعلوماتية:

المادة (٢١) من قانون مكافحة جرائم تقنية المعلومات المصري / تقضي بمعاقبة كل من تسبب متعمدا في إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها بالحبس مدة لا تقل عن ستة شهر، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين.**([37])**

ولم يذهب المشرع السعودي بعيداً عن ذلك، فقد تناول في الفقرتين الثانية والثالثة من المادة الخامسة النص على ذات الأفعال الوارد ذكرها بالتقنين المصري وزاد عليها واعتبرها من قبيل الأفعال الإجرامية الخطرة واجبة العقاب.

وقد سايرهم في ذلك المشرع الكويتي في المادة الرابعة منه ولكنه كان غير موفق في الصياغة القانونية، حيث يؤخذ عليه في هذه المادة إغفال وعدم ذكر بعض الأفعال والسلوكيات التي تؤدي إلى وقوع الجريمة مثل فعل التشويش أو محاولة الحد من كفاءة عملها أو إعاقتها أو اعتراض عملها أو قيام الجاني بإجراء معالجة إلكترونية للبيانات الخاصة بالشبكة المعلوماتية بدون وجه حق أسوة بما فعله المشرع المصري على النحو المتقدم .وبالنسبة لموقف المشرع

الإماراتي أيضاً فلم يختلف كثيراً عما ذهب إليه المشرع الكويتي من عدم التوسع في ذكر الأفعال والانتهاكات التي تمثل اعتداء على سلامة الشبكة المعلوماتيةوأغفل أيضاً ذكر البعض منها .

المطلب الثانى

جرائم الاعتداء على حرمة الحياة الخاصة([38])

لايزال المشرع المصري حريصاً على حماية الحقوق والحريات حرصاً عظيماً لاسيما حق الإنسان في الحياة الخاصة، والعمل على مواجهة كل ما ينطوي عليه استخدام وسائل التقنية الحديثة من انتهاكات وتهديدات للحق في الخصوصية، فلم يكتفي المشرع المصري بإفراغ ذلك الاهتمام في نصوص قانونية، وإنما تخطي ذلك إلى أن ضمنه في نصوص دستورية ضمن نصوص الدستور المصري لعام ٢٠١٤ ، وعمل على إحاطتها بحماية خاصة ضد أية انتهاكات قد تحدث من وسائل التقنية المعلوماتية، ومنها الاهتمام بالحفاظ على سرية المحادثات والمراسلات البريدية وغيرها من وسائل الاتصالات والمعلومات، وحظر رقابتها أو وقفها أو تعطيلها أو الحد من كفاءتها أو التنصت عليها إلا بأمر قضائي، نظراً لما تسببه هذه التعديات من تهديد لمنظومة الاقتصاد والأمن القومى وبإصدار قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨

خصص المشرع المصري فصلاً خاصاً لمكافحة الجرائم التقنية التي تقع على حرية الإنسان وانتهاك خصوصيته تضمن في المادة ٢٥ منه تجريم كل فعل ينطوي على اعتداء يقع على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهاك حرمة الحياة الخاصة، أو القيام بإرسال رسائل الإلكترونية لشخص معين بكثافة دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع لكتروني لترويج السلع أو الخدمات دون موافقة صاحب الشأن، أو نشر معلومات أو أخبار أو صور وما في حكمها عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات يترتب عليها أن تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيح([39]).

وهذا وقد سعت أغلب التشريعات المقارنة أيضاً لحماية هذه الخصوصية إلا أن البين أن اهتمامها كان اهتماماً محدوداً بالمقارنة بما آتاه المشرع المصري، فمنها المشرع السعودي الذي تناول في المادة الثالثة، والفقرة الأولي من المادة الخامسة النص على حماية حرمة الحياة الخاصة وحق الإنسان في الخصوصية من أفعال التنصت على المراسلات البريدية الالكترونية أو اعتراضها، وكذا الدخول غير المشروع إلى مواقع إليكترونية بهدف التهديد أو الابتزاز أو إتلاف هذه المواقع والتصاميم أو استخدام الهواتف النقالة المزودة كاميرات في الإساءة والمساس بالحياة الخاصة والتشهير بالغير وإلحاق الضرر به، إضافة لما جاء بالمادة السادسة من حماية حق الإنسان من إنتاج ما من شأنه المساس بحرمة الحياة الخاصة([40]).

وبالنسبة للتشريع الكويتي فقد تناول النص على هذه الحماية التشريعية للحياة الخاصة في الفقرة الثالثة من المادة الثانية والتي تضمنت تشديد العقوبة إذا ما وقعت هذه الاعتداءات على بيانات أو معلومات شخصية، وفي الفقرة الرابعة من المادة الثالثة قام بمعاقبة كل من استعمل

الشبكة المعلوماتية أو استخدم وسيلة من وسائل تقنية المعلومات في تهديد أو ابتزاز شخص طبيعي أو اعتباري لحمله على القيام بفعل أو الامتناع عنه .وضاعف من حد العقوبة إذا كان التهديد بارتكاب جناية أو بما يعد مساسا بكرامة الأشخاص أو خادشا للشرف والاعتبار أو السمعة وفي المادة الرابعة تناول التأكيد على حظر وتجريم التصنت أوالتجسس أو إعاقة للوصول إلى مواقع أو بيانات، أو اعتراض أية مراسلات تتم عن طريق الشبكة المعلوماتية أو وسيلة من وسائل التقنية المعلوماتية، أو قام بإفشائها أو نشرها للعامة، وكل ذلك يعد من قبيل الاعتداءات الواقعة على الحقوق الخاصة للأفراد([41]).

ويعتبر المشرع الإماراتي من أكثر التشريعات المقارنة اهتماماً بحماية حرمة الحياة الخاصة أسوة بالمشرع المصري، وقنن لها نصوصاً متعددة منها ما جاء بالفقرة الأولي من المادة ٢١ من القانون رقم ٥ لسنة ٢٠١٢ وتعديلاته التي تضمنت تجريم كل فعل يمثل اعتداء لخصوصية شخص ما يتم بواسطة استخدام احدي وسائل تقنية المعلومات أو الشبكات المعلوماتية، وقد عددت هذه الفقرة الطرق التي تمثل فعل اعتداء منها استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية، وكذا التقاط صور الغير أو إعداد صور إلكترونية أن نقلها أو كشفها أو نسخها أو الاحتفاظ بها . كما أدخل المشرع من ضمن هذه الأفعال نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية، وقد عاقب مرتكبي هذه الأفعال بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز خمسمائة ألف درهم أو بإحدى هاتين العقوبتين.

وفي الفقرة الثانية من ذات المادة ٢١ ضاعف المشرع من حد العقوبة في حالة قيام الجاني باستخدام نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، لإجراء أي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر، أو الاعتداء على خصوصيته أو انتهاكها أو قيامه بدون تصريح باستخدام أي شبكة معلوماتية، أو موقعا إلكترونيا، أو وسيلة تقنية معلومات لكشف معلومات سرية حصل عليها بمناسبة عمله أو بسببه.

ويتبين مما سبق أن المشرع المصري يعد من أفضل مشرعي دول العالم حرصاً على حماية حرمة الحياة الخاصة، وتبعه في ذلك المشرع الإماراتي، ونشيد لهما بحسن الصياغة القانونية لهذه النصوص العقابية([42]).

ولقد حظي هذا الحق باهتمام كبير سواء من جانب الهيئات والمنظمات الدولية أو من جانب الدساتير والنظم القانونية ، فعلى الصعيد الدولي نجد أن هذا الاهتمام يبرز في صورة اتفاقيات دولية كالإعلان العالمي لحقوق الإنسان الصادر من الجمعية العامة للأمم المتحدة بموجب قررها رقم 217 المؤرخ في 1948/12/10 م في المادة (12) منهٍ

ولقد تضاعف الاهتمام بهذا الحق نظرا لما يتعرض له من مخاطر تحيط به وتهدده أبرزها التقدم التكنولوجي والإعلامي و المعلوماتى الملحوظ والذي كان له دور كبير في اقتحام حصون

هذا الحق واختراق حواجزه وتسلق أسواره ، الأمر الذي يقتضي تدخل المشرع لحمايته بالأسلوب الذي يتفق وطبيعة هذه الأخطار .

فضلا عن المؤتمرات الدولية التي انعقدت في أنحاء العالم لبحث أفضل الوسائل لحماية هذا الحق([43]) كالقرار الصادر من المؤتمر الدولي لحقوق الإنسان المنعقد في طهران في الفترة من 22 إبريل إلى 13 مايو 1968والذي هدف في مضمونه إلى حماية حق الإنسان في حياته الخاصة ، وأيضا مؤتمر حقوق الإنسان المنعقد خلال العام الدولي لحقوق الإنسان 1968م في مونتريال بكندا الذي وجه الأنظار إلى الأخطار الجديدة الناتجة عن التطورات التقنية والعلمية على هذا الحق مثل التجسس الإلكتروني ، أضف إلى ذلك مؤتمر الحق في حرمة الحياة الخاصة الذي انعقد بمدينة الإسكندرية خلال الفترة من 4-1987/6/6م.

وفى سلطنه عمان فإن الاهتمام بهذا الحق يبرز من خلال ما نصت عليه في الدساتير والنظم السياسية للدول كالنظام الأساسي لسلطنة عمان الصادر بالمرسوم السلطاني رقم 96/101 في المواد 18،27،30 منه .والمواد 45،57 من الدستور المصري1971م ، والمواد7 ، 10 ، 15 من الدستور الأردني 1952م ، والمواد 11 ، 29 ، 30 ، 31 ، 39 من الدستور الكويتي.

بالإضافة إلى ذلك نجد أن غالبية الدول([44]) ومن خلال تشريعاتها الوطنية قد أصبغت حمايتها الجنائية لهذا الحق كالمادة 262من القانون الجزاء العماني والمواد226-1 إلى 226-7 من قانون الفرنسي الجديد والمواد 309مكرر و309 مكرر(أ) من قانون العقوبات المصري.

ولم تترد المحكمة الدستورية لألمانيا الاتحادية في قرار مهم لها في شأن الاحصاء القومي من اعتبار قضية المعلومات على أنها بالنسبة للأفراد قضية " حق تحديد مصير بالنسبة للمعلومات " ، حيث أوضحت المحكمة بأن عدم التقيد والضبط في الوصول إلى المعلومات والبيانات الفردية يعرض للخطر وبشكل فعلي ، جميع الحقوق المحمية في الدستور وبشكل فعلي ، جميع الحقوق المحمية في الدستور.

أما على صعيد التشريع فقد شهدت أوروبا ، تطوير هذه الفكرة ضمن حزمة شاملة من مبادئ السلوك والممارسات المقبولة ، أهمها تأكيد الاستخدام العادل والمنصف للبيانات الشخصية ، والتدخل بالحدود الدنيا ، وتقييد وتضييق أغراض استخدام البيانات وحصر الاستخدام في غرض الجمع([45]) .

ففي ألمانيا ظهرت اول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في ولاية هيس بالمانيا، لكن هذه المعالجة لا تعد قانونا متكاملا لاعتبارات عديدة اولها انه ليس قانون دولة ، وقد تبعه سن اول قانون وطني (متكامل) في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم المانيا على المستوى الفدرالي عام 1977 ثم فرنسا عام 1978 وفي عام 1981 وضع مجلس أوروبا اتفاقية حماية الافراد من مخاطر المعالجة الالية للبيانات الشخصية، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا ارشاديا لحماية الخصوصية ونقل البيانات الخاصة ، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات ، وهذه القواعد تصف البيانات والمعلومات الشخصية على انها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر ثم وفي خطوة متطورة على المستوى

التشريعي الاقليمي ، بل وذات اثر عالميا ، اصدر الاتحاد الأوروبي الامر التشريعي الخاص بحماية البيانات ونقلها عبر الحدود لعام 1995 ، الذي مثل مرحلة جديدة في اعادة تنظيم خصوصية المعلومات ادت الى اعادة وضع العديد من دول أوروبا تشريعات جديدة او تطوير تشريعاتها القائمة في هذا الحقل ، بل اثر فيما تضمنه من معايير في حقل نقل البيانات خارج الحدود لجهة في سعي العديد من دول العالم خارج نطاق اوروبا الى التواؤم مع ما قرره هذا الأمر التشريعي.([46])

المبحث الثالث

ماهية أمن المعلومات

الأمن اصطلاحا : اطمئنان الفرد والأسرة والمجتمع على أن يحيوا حياة طيبه بالدنيا ولا يخافوا على أموالهم ودينهم ونسلهم من التعدي عليهم بدون وجه حق([47]) .

المعلومات : هي البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد ، لأغراض اتخاذ القرار أو هي البيانات التي أصبح لها قيمة بعد تحليلها

أمن المعلومات: هو العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

ويعرف البعض أمن المعلومات بانه ([48])السيطرة التّأمة على المعلومات، من حيث تحديد من سيستلم هذه البيانات، وتحديد صلاحيّات الوصول إليها، واستخدام مجموعة من التقنيّات من أجل ضمان عدم اختراقها من قبل أي جهة، وتتضاعف أهميّتها من الحفاظ على الخصوصيّة، إلى الحفاظ على بيانات هامّة مثل حسابات العملاء في البنوك.

كما يعرف بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها([49]) .

ومن زاوية تقنية ، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية .

ومن زاوية قانونية ، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة ، وهو هدف وغرض تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت)([50]) .

وبالتالى يمكن النظر الى امن المعلومات على انه : مجموعة العمليات والإجراءات والأدوات التي تتخذها القطاعات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها ووسائطها من وصول غير المصرح لهم ، سواء في ذلك من هم من داخل القطاع أو من خارجه([51]).

المطلب الاول

اهداف أمن المعلومات وعناصره

1- اهداف أمن المعلومات : يسعى امن المعلومات الى ضمان توفر العناصر التالية لاية معلومات يراد توفير الحماية الكافية لها ([52]):-

الخصوصية أو السرية:

وهي الخصوصية للمعلومات المتعلقة بالعملاء أو بالمنظمة بحيث تكون بعيد عن وصلو غير المصرح لهم بالاطلاع عليها. ومن الأمثلة المستخدمة للحصول على الخصوصية – نظام التشفير، وهو من الأمثلة المهمة التي توفر مستوى عالٍ من الأمن للمعلومات مع المحافظة على المرونة في تداول تلك البيانات([53]) .

السلامة للمعلومات والأنظمة :

بحيث يمكن التأكد من عدم تعرضها لأي نوع من التغيير الغير مصرح به، وبعبارة أخرى فإن البيانات لا يمكن أن يحدث لها استحداث أو تغيير أو حذف من غير تصريح، وكذلك تعني أن البيانات المخزنة في أحد أجزاء جداول قواعد البيانات متوافقة مع ما يقابلها من البيانات المخزنة في جزء آخر من قواعد البيانات. مثال ذلك: يمكن أن تتغيب سلامة البيانات في قواعد البيانات عند حدوث انقطاع مفاجئ للكهرباء التي تغذي جهاز الخادم، أو عند عدم إقفال قاعدة البيانات بشكل صحيح، وكذلك بسبب حذف لمعلومة بطريقة الخطأ من قبل أحد الموظفين، وقد يحصل الخلل أيضا بسبب فيروس.

التوفر بشكل دائم للمعلومات والأنظمة الحاسوبية والعمليات الأمنية :

بحيث تعمل بشكل سليم عند الحاجة لها، وذلك بعد تطبيق العمليات الخاصة بأمن المعلومات.

ولتحقيق هذه الأمور، نحتاج لاستخدام مجموعة من المقاييس وهي:

1- (التحكم بالوصول)

2- (إثبات الصلاحيات)

3- (التدقيق)

وهذه الأمور الثلاث السابقة هى الأمر الأساسي لفهم أمن الشبكات وأمن الوصول للبيانات, وتستخدم هذه الأمور الثلاثة بشكل يومي في حماية البيانات الخاصة وحماية الأنظمة من التخريب المتعمد والغير متعمد. وهذه المفاهيم السابقة تدعم مفاهيم الأمن الخصوصية والسلامة والتوفر([54]) .

2- عناصر أمن المعلومات([55]) :

ان ضمان عناصر أمن المعلومات كلها او بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها ، فليس كل المعلومات تتطلب السرية وضمان عدم

الافشاء ، وليس كل المعلومات في منشأة واحدة بذات الاهمية من حيث الوصول لها او ضمان عدم العبث بها ، لهذا تنطلق خطط أمن المعلومات من الاجابة عن سلسلة تساؤلات متتالية :-

1- ما الذى يجب ان نحميه؟ واجابة هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث اهمية الحماية ، اذ تصنف المعلومات تبعا لكل حالة على حده ، من معلومات لا تتطلب الحماية ، الى معلومات تتطلب حماية قصوى

2- ما هي المخاطر التي تتطلب هذه الحماية ([56])؟ وتبدا عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية او يهدد امنها ، ابتداء من قطع مصدر الكهرباء عن الكمبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد او اكثر من وسائل الاختراق عبر نقاط الضعف ، مرورا باساءة الموظفين استخدام كلمات السر العائدة لهم ، ويصار الى تصنيف هذه المخاطر ضمن قوائم تبعا لاساس التصنيف ، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها ، ومن حيث غرض المتسببين بهذه المخاطر ، ومن حيث اثرها على نظام الحماية وعلى المعلومات محل الحماية. وهو ما سنقف لاحقا عليه بشكل تفصيلي .

3- ما هى وسائل الحماية : وهنا تجد كل منشاة وكل هيئة طريقتها الخاصة في توفير الأمن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات المخصوصة التي تم تحديدها وبحدود امكاناتها المادية والميزانية المخصصة للحماية ، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغا بها الى حد يؤثر على عنصر الأداء في النظام محل الحماية([57]) .

وفي بيئة المعلومات ، فمن الطبيعي مثلا ان نضع على جهاز الكمبيوتر الشخصي كلمة سر للوصول الى الملفات الهامة او حتى للنظام كله وان لا نعطي الكلمة لاحد ، وان نضع برنامجا او اكثر لمقاومة الفيروسات الإلكترونية الضارة ، ونراعي إجراءات مقبولة في حماية الدخول الى شبكة الإنترنت والتأكد من مصدر البريد الإلكتروني مثلا([58]) .

فإذا كان الكمبيوتر خاص بدائرة او منشاة ويضم بيانات هامة ومصنف انها سرية ، كان لزاما زيادة إجراءات الأمن ، فمثلا يضاف للنظام جدران نارية تحد من دخول اشخاص من الخارج وتمنع اى اعتداءات قد يتعرض لها النظام او الموقع المعلوماتي ، واذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الافشاء ، تكون تقنيات التشفير مطلوبة بالقدر المناسب([59]) .

بمعنى ان إجراءات الحماية تنطلق من احتياجات الحماية الملاءمة ، فان زادت عن حدها أمست ذات اثر سلبي على الأداء ، فاصبح الموقع او النظام بطيئا وغير فاعل في أداء مهامه الطبيعية ، وان نقصت عن الحد المطلوب ، ازدادت نقاط الضعف واصبح اكثر عرضة للاختراق الداخلي والخارجي . فإذا فرغنا من اختيار وسائل الحماية التقنية واستراتيجياتها الإدارية والادائية الملائمة ، انتقلنا بعدئذ الى التساؤل الاخير.

4- ما هى خطط مواجهة الأخطار عند حصولها : وتتضمن مراحل متتالية ، تبدأ من مرحلة الإجراءات التقنية والادارية والاعلامية والقانونية اللازمة عند حصول ذلك ، ومرحلة

إجراءات التحليل لطبيعية المخاطر التي حصلت وسبب حصولها وكيفية منع حصولها لاحقا. واخيرا إجراءات التعافي والعودة الى الوضع الطبيعي قبل حصول الخطر مع مراعاة تنفيذ ما اظهره التحليل عن كيفية حصول المخاطر وضمان عدم حصولها ([60]).

المطلب الثانى

المخاطر والاعتداءات في بيئة المعلومات

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي([61]) :-

• **الأجهـزة :-** وهي كافة المعدات والادوات المادية التي تتكون منها النظم ، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها .

• **البرامــج :-** وهي الاوامر المرتبة في نسق معين لانجاز الاعمال ، وهي اما مستقلة عن النظام او مخزنة فيه .

• **المعطيـات :-** انها الدم الحي للأنظمة ، وما سيكون محلا لجرائم الكمبيوتر ، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها ، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم .

والمعطيات قد تكون في طور الادخال او الاخراج او التخزين او التبادل بين النظم عبر الشبكات ، وقد تخزن داخل النظم او على وسائط التخزين خارجه .

• **الاتصـالات :-** وتشمل شبكات الاتصال التي تربط اجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا ، وتتيح فرصة اختراق النظم عبرها كما انها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي.

ومحور الخطر ، الانسان ، سواء المستخدم او الشخص المناط به مهام تقنية معينة تتصل بالنظام ، فادراك هذا الشخص حدود صلاحياته ، وادراكه اليات التعامل مع الخطر ، وسلامة الرقابة على انشطته في حدود احترام حقوقه القانونية ، مسائل رئيسة يعنى بها نظام الأمن الشامل ، تحديدا في بيئة العمل المرتكزة على نظم الكمبيوتر وقواعد البيانات([62])

المبحث الرابع

حماية امن المعلومات فى الدستور والقانون والمواثيق الدولية

على الجانب التشريعي فقد أتاحت كافة الدساتير والمعاهدات والاتفاقيات العالمية والمحلية للإنسان الحرية الكاملة في استخدام وسائل التقنية المعلوماتية وتبادل البيانات والمعلومات ووسائل التواصل الاجتماعي إلا أن هذه الحرية لا ينبغي أن تجعل من الانترنت ووسائل التقنية الحديثة بيئة متحررة من القواعد والنصوص القانونية الحاكمة والمنظمة لها([63]) ، فإلى جانب المزايا العديدة التي خلفها هذا التطور التكنولوجي الحديث، أفرز لنا الكثير من الجرائم والتعديات التي تختلف في صفاتها وأشكالها وأثارها عن الجرائم التقليدية، وأصبحت تمثل تهديداً مباشراً وواضحاً للأمن والاستقرار المحلي والعالمي، وعائقاً يحول دون إتمام عملية

التطوير والتنمية، ولم تقتصر عواقبه وآثاره على المستوي الفردي بل امتدت لتهدد المجتمع الدولي بأكمله، خاصة وأن هذه الطائفة من الجرائم تتميز بأنها معقدة للغاية لتنوعها وسهولة ارتكابها وقدرة الجناة على التخفي والهرب، مما يصعب معه اكتشافها، واثبات أدلتها، وضبط مرتكبها، وإسنادها إليهم.([64])

وإزاء ذلك حملت العديد من الدول على عاتقها لواء البحث في هذا الجانب، وحرصت على تطوير نظم المكافحة التشريعية لديها بإدخال نصوص تشريعية عقابية وإجرائية تتوافق مع ظاهرة الإجرام التقني الحديثة، ولم تكتفي بذلك فحسب بل قامت بسن تشريعات خاصة مستقلة تتعلق بهذا الشأن .

المطلب الاول

الحماية الدستورية لامن المعلومات

حظى الحق فى الخصوصية أو حرمة الحياة الخاصة بعناية خاصة في الدستور المصري الصادر عام 2014 ، فاعتبره حقاً من الحقوق الدستورية المطلقة، حيث نصت المادة 57 منه على أن" :للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون.([65])

كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك."

ولم يقف عند هذا الحد، بل وفر الحماية ضد الاعتداء علي هذا الحق أو المساس به، فقررت المادة 99 من الدستور أن: "كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم، وللمضرور إقامة الدعوى الجنائية بالطريق المباشر([66])."

وفى سبيل التأكيد على أهمية حماية الحق فى الخصوصية، وهو ما ينصرف بالطبع للبيانات الشخصية، ذهبت المحكمة الدستورية العليا المصرية - فى حكمها الصادر بجلسة 15نوفمبر 1996إلي أن هناك " ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي دوماً ألا يقتحمها أحد ضماناً لسريتها وصوناً لحرمتها، فلا يكون اختلاس بعض جوانبها مقبولاً.([67])

وكذلك بما ينبغي أن يستقل به كل فرد من سلطة التقرير فيما يؤثر في مصيره، وتبلور هذه المناطق جميعها التي يلوذ الفرد بها، مطمئناً لحرمتها، وامتناع إخضاعها لأشكال الرقابة وأدواتها على اختلافها.

والحق في أن تكون للحياة الخاصة تخومها، باعتبار أن صونها من العدوان أوثق اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة، وأكفل للحرية الشخصية التي يجب أن يكون نهجها متواصلاً ليوائم مضمونها الآفاق الجديدة التي ترنو الجماعة إليها."

كذلك احتوى قانون حماية البيانات الشخصية رقم 151 لسنة 2020 على استثناءات، تسمح لبعض الجهات بانتهاك خصوصية المواطنين، إذ تنص المادة (3) من القانون على استثناء بعض الجهات من أحكام القانون، من أهمها: "جهات الأمن القومي و"البنك المركزي المصري والجهات الخاضعة لإشرافه ورقابته".

ويماثل هذا الاستثناء ما هو ممنوح لجهات الأمن القومي في قانون مكافحة جرائم تقنية المعلومات فيما يتعلق بالحصول على بيانات المستخدمين.

المطلب الثانى

الحماية القانونية لامن المعلومات

حرص المشرع المصري على مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العالم في العصر الحديث، بإصداره العديد من التشريعات اللازمة لمواجهة هذا الغزو التقني ودخول الرقمية فضائها المعلوماتى([68])، ومن هذه التشريعات قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ م الخاص بتأمين نقل وتبادل المعلومات ، والقانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة المعلومات الدولية" الإنترنت ، القانون رقم لسنة ١٩٩٤ بشأن الأحوال المدنية([69]) .

هذا إلى جانب العديد من القرارات التنظيمية التي أصدرتها وزارة الاتصالات بهدف حماية تقنية المعلومات والاتصالات .

وقد أنشأت مصر بموجب قرار مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ مجلس أعلي للأمن السيبرانى ، لتكون مهمته وضع إستراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها و أصدر السيد رئيس الجمهورية قرار بشأن الموافقة على انضمام مصر إلى الاتفاقية العربية (رقم ٢٧٧ لسنة ٢٠١٤ لمكافحة الجريمة المنظمة عبر الحدود الوطنية الموقعة في القاهرة ٢٠١٨ .

القانون رقم ١٧٥ لسنة ٢٠١٨:

بشأن مكافحة جرائم تقنية المعلومات، (ولائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠ ولم يكن هو الخطوة الأولي في مجال التشريع المعلوماتى، بل سبقه العديد من الاجتهادات والتشريعات التي تناولت تنظيم مجال التقنية المعلوماتية كان من بينها قانون حماية الملكية الفكرية، وقانون التوقيع الالكترونية، وقانون تنظيم الاتصالات وتكنولوجيا المعلومات.

كذلك لم يكتفى بهذا القدر ففى قانون العقوبات، أفرد المشرع عقوبة خاصة لكل من يعتدى على حرمة الحياة الخاصة للمواطن([70]) وهى عقوبة الحبس لمدة لا تزيد على سنة([71])، كما

يعاقب كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصاً عليه بطرق غير مشروعة أو كان بغير رضاء صاحب الشأن، كما يعاقب كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها لحمل شخص على القيام بعمل أو الامتناع عنه بالسجن مدة لا تزيد على خمس سنوات (م 309 مكرر أ عقوبات.)

كما شدد المشرع العقوبة على من يفشي سر خصوصي أؤتمن عليه بحكم وظيفته كالأطباء والجراحين أو الصيادلة والقوابل يعاقب بالحبس مدة لا تزيد علي ستة أشهر أو بغرامة (م310عقوبات.)([72])

وفى قانون الأحوال المدنية رقم 143 لسنة 1994 :

تشير المادة 13منه إلى أن" "تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الملحقة سرية، ولا يجوز الاطاع عليها أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون ووفقا لأحكامه.

وتعتبر البيانات أو المعلومات أو الإحصائيات المجمعة التي تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين سرًا قوميًا، ولا يجوز الاطاع عليها أو نشرها إلا لمصلحة قومية أو علمية وبإذن كتابي من مدير قطاع الأحوال المدنية أو من ينيبه وفقا للأوضاع و الشروط التي يحددها القانون واللائحة التنفيذية.

كما حرص قانون البنك المركزى والجهاز المصرى الصادر عام 2020 :

على سرية بيانات وحسابات العملاء، حيث تنص المادة 140 منه على أن تكون جميع بيانات العملاء وحساباتهم وودائعهم وأماناتهم وخزائنهم في البنوك وكذلك المعلامات المتعلقة بها سرية، ولا يجوز الاطاع عليها أو إعطاء بيانات عنها بطريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب أو الوديعة أو الأمانة أو الخزينة أو من أحد ورثته أو من أحد الموصى لهم بكل هذه الأموال أو بعضها، أو من نائبه القانوني أو وكيله أو بناء على حكم قضائي أو حكم تحكيم.

الحق في الحصول على المعلومات والخصوصية في القانون المصري:

تنوعت أشكال الحماية التي خصصها قانون العقوبات للحياة الخاصة للأفراد، وللمعلومات اللصيقة بخصوصياتهم واعتبرها المشرع خارج نطاق الحق في الحصول على المعلومات.

فخصص حماية خاصة لمراسلات الأشخاص حين قضت بعقوبة الحبس والغرامة التي لا تزيد على خمسمائة جنيه والعزل من الوظيفة لموظف الحكومة أو البوستة الذي يقوم بإخفاء أو فتح المكاتبات الخاصة بالمتعاملين مع البوستة أو يقوم بتسهيل ذلك للغير، وذلك ينطبق على التلغرافات([73]).

ويتبين من هذا النص أن وقوع الجريمة مقيد بصفة مرتكبها، وهو أن يكون موظفا عموميا سواء ارتكب الجريمة بنفسه أو سهل لآخر القيام بها ، وكذلك حظر قانون العقوبات حظراً

مطلقا نشر أية معلومات أو أخبار متعلقة بالتحقيقات أو المرافعات في دعاوى الطلاق أو التفريق أو الزنا، وقد جاء هذا الحظر دون أن يتوقف على قرار من سلطة التحقيق أو المحاكمة، وبالتالي لا يؤثر ذلك إذا تذرع الناشر بعدم العلم، انطلاقا من قاعدة أن العلم بالقانون مفترض للكافة ([74])

وقد رأى بعض الفقه أن الحكمة من حظر النشر في هذه الدعاوى انها ذات خصوصية شديده وينطوى نشر ما يجرى فيها من تحقيقات أو مرافعات على طرح خصوصيات الأفراد على الجمهور، حيث لا توجد مصلحة عامة يمكن أن تتحقق من وراء النشر ([75])

وعاقبت المادة 309 مكرر من قانون العقوبات بالحبس ومصادرة الأجهزة والأدوات المستخدمة ومحو التسجيلات المتحصلة من الجريمة كل من ارتكب إحد صور الاعتداء على حرمة الحياة الخاصة للمواطنين التي قسمها هذان نص إلى نوعين:

1-استراق السمع أو التسجيل أو النقل عن طريق أي جهاز لمحادثات جرت في مكان خاص أو عن طريق التليفون.

2-التقاط صورة لشخص في مكان خاص.

إلا أن هذه الجريمة تضمنت سببا من أسباب الإباحة حيث نصت الفقرة الثانية على مشروعية هذه الأفعال إذا حدثت أثناء اجتماع على مرأى ومسمع من الحاضرين بشرط رضائهم.

كذلك نصتّ المادة(309 مكرر (أ) على أن:يعاقب بالحبس كل من أذاع أو سهل إذاعة أو أستعمل ولو في غير علانية تسجيلا أو مستندا متحصلا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن.

ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه.

ويعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة في هذه المادة اعتمادا على سلطة وظيفته([76]).

ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها.

والمادتين(309 مكرر و 309 مكرر (أ) اقتصر نطاق الحماية المقرر بهما على المحادثات التي تسجل عن طريق جهاز من الأجهزة أيا كان نوعه وكذلك الصور، ومع التطور التكنولوجي لوسائل الاطلاع على وحفظ و تداول المعلومات، نجد قصور شديد خاصة في مواجهة نظم حفظ المعلومات الموجودة لدى الأجهزة الحكومية، وشركات الاتصالات وغيرها من الأجهزة التي تحتفظ بقواعد بيانات للأفراد، والتي غالبا ما يتم اقتحامها من قبل الأجهزة الأمنية والسلطات المختلفة، كالوضع في مصر، وعلى الرغم من معالجة قانون الاتصالات لهذه المسألة وتوفير حماية لخصوصية بيانات الأفراد التي لدى الأجهزة والشركات إلا أن قانون العقوبات يشوبه النقصان في معالجة هذه الأمور باعتباره القانون العقابي العام([77]).

ويثور التساؤل حين ترتبط المعلومات الخاصة بالأفراد بشئون المصلحة العامة، ويذهب جانب من الفقه القانوني في هذا الصدد إلى أنه إذا تعلق الأمر الخاص بالمصلحة العامة ويؤثر فيها، فإنه يجوز التعرض للمعلومات المتصلة بالحياة الخاصة بالقدر اللازم لهذا الارتباط، وإباحة التداول والنشر تنحصر في الأعمال التي يأتيها الموظف دون الآراء والمحادثات التي جرت في مكان خاص أو عن طريق التليفون، مهما كانت طبيعة الحديث([78])

0وهو ما جاء في متن المادة 21 من قانون تنظيم الصحافة رقم 96 لسنة 1996 التي نصت على أنه " لا يجوز للصحفي أو غيره أن يتعرض للحياة الخاصة للمواطنين، كما لا يجوز له أن يتناول مسلك المشتغل بالعمل العام أو الشخص ذي الصفة النيابية العامة أو المكلف بخدمة عامة إلا إذا كان التناول وثيق الصلة بأعمالهم ومستهدفا المصلحة العامة.

أيضا ألزم قانون العقوبات طائفة من الناس بالحفاظ على سرية المعلومات التي يتلقونها بحكم وظائفهم وهذا ما نصت عليهم المادة 310 التي حددت بعض الوظائف على سبيل المثال كالأطباء والصيادلة والجراحين والقوابل، بأن على هؤلاء عدم إفشاء الأسرار التي تودع لديهم بمقتضى وظائفهم إلا في الأحوال التي يلزمهم فيها القانون بذلك، وقد حددت المادة عقابا لمخالف ذلك الحظر بالحبس ستة شهور وغرامة لا تزيد عن خمسمائة جنيه.

وهو نفس ما اتجه إليه قانون الإجراءات الجنائية([79]) في المادة 75 منه حيث اعتبر إجراءات التحقيق والنتائج التي تسفر عنها من الأسرار، و ألزم قضاة التحقيق وأعضاء النيابة العامة ومساعديهم من كتاب وخبراء وغيرهم ممن يتصلون بالتحقيق أو يحضرونه بسبب وظيفتهم أو مهنتهم بعدم إفشائها، وقد أسندت تلك المادة العقاب على مخالفتها إلى المادة 310 من قانون العقوبات.

كذلك ألزمت المادة 58 من قانون الإجراءات الجنائية([80]) مأموري الضبط القضائي بالحفاظ على أسرار المهنة عما يصل إلى علمهم بسبب التفتيش من معلومات عن الأشياء والأوراق المضبوطة .

وقضت الماده 146 من القانون رقم 157 لسنة 1981 بشان الضرائب على الدخل على أن كل شخص يكون له بحكم وظيفته أو اختصاصه أو عمله شأن في ربط أو تحصيل الضرائب المنصوص عليها في هذا القانون أو في الفصل فيما يتعلق بها من منازعات ملزم بمراعاة سر المهنة .

وحظرت المادة الخامسة من القرار بقانون رقم 205 لسنة 1990 في شأن سرية الحسابات بالبنوك، على رؤساء وأعضاء مجالس إدارة البنوك ومديريها أو العاملين إعطاء أو كشف أية معلومات أو بيانات عن عملاء البنوك أو تمكين الغير من الاطلاع عليها في غير الحالات التي يبيح فيها القانون`ذلك([81])

ومن الأنظمة القانونية المستحدثة في التشريع المصري هو قانون تنظيم الاتصالات رقم 12 لسنة 2003 الذي أفرد حماية للحق في خصوصية المعلومات والبيانات الخاصة بمستخدمي الاتصالات بموجب المادة 73 منه والتي عاقبت بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة

لا تقل عن خمسة آلاف جنيه و لا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بإحدى الأفعال الآتية:([82])

1- إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانوني في ذلك.

2-إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.

3-الامتناع عمدا عن إرسال رسالة اتصالات بعد تكليفه بإرسالها.

4- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق.

إلا أن الحماية المقررة للحق في الخصوصية مقيدة، حيث إنه وفقان لنص المادة 67 من قانون الاتصالات للسلطات المختصة في الدولة أن تخضع لإدارتها جميع خدمات وشبكات اتصالات أي مشغل أو مقدم خدمة وأن تستدعي العاملين لديه القائمين على تشغيل وصيانة تلك الخدمات والشبكات وذلك في حالة حدوث كارثة طبيعية أو بيئية أو في الحالات التي تعلن فيها التعبئة العامة طبقا لأحكام القانون رقم 87 لسنة 1960 وأية حالات أخرى تتعلق بالأمن القومي.

الأمن القومي وحماية امن المعلومات([83]) :.

يعد الأمن القومي من الموانع الأساسية لتداول المعلومات ليس في مصر وحدها، بل في أنظمة قانونية كثيرة، وبالنسبة للتشريع المصري ،فلم يحدد تعريفا واضحا لماهية الأمن القومي الجدير بالحماية عبر حظر نشر معلومات معينة أو الحصول عليها إذا تعارض ذلك مع مقتضيات الحماية التي يكفلها له القانون، وقد عرفت المادة 1 من قانون الاتصالات رقم 10لسنة 2003 الأمن القومي بأنه كل ما يتعلق بشئون رئاسة الجمهورية والقوات المسلحة والإنتاج الحربي ووزارة الداخلية والأمن العام وهيئة الأمن القومي وهيئة الرقابة الإدارية، والأجهزة التابعة لهذه الجهات، كما عرفت أجهزة الأمن القومي بأنها رئاسة الجمهورية ووزارة الداخلية وهيئة الأمن القومي وهيئة الرقابة الإدارية وهذا المفهوم الذي تبناه قانون الاتصالات لمصطلح الأمن القومي توسع في نطاق التطبيق، إذ إنه لم يحدد أنشطة محددة لرئاسة الجهورية أو وزارة الداخلية على سبيل المثال يمكن إدراجها تحت هذا المفهوم ،بل جاء التعريف عاما شاملا لكل ما هو متعلق بأنشطة هذه الأجهزة.

وقد عرفت محكمة القضاء الإداري الأمن القومي بأنه قدرة الدولة على حماية أراضيها وقيمها الأساسية والجوهرية من التهديدات الخارجية، وبخاصة العسكرية منها، انطلاقا من أن تأمين أراضى الدولة ضد العدوان الأجنبي، وحماية مواطنيها ضد محاولات إيقاع الضرر بهم وبممتلاكاتهم ومعتقداتهم وقيمهم موقيمهم، هو دافع الولاء الذي يمنحه الشعب للدولة بالعقد الاجتماعي المبرم معه"

كما وضحت المحكمة الأبعاد المتعددة للأمن القومي فعرفت البعد السياسي للأمن القومي بأنه "ذو شقين داخلي وخارجي، ويتعلق البعُد الداخلي بتماسك الجبهة الداخلية وبالسلام الاجتماعي

والمواطنة وتراجع القبلية والطائفية، أما البعد الخارجي فيتصل بتقدير أطماع الدول العظمى في أراضى الدولة، و البعُد الاقتصادي فيتعلق بالإستراتيجية الوطنية التي تعنى بتنمية واستخدام كافة موارد الدولة لتحقيق، أهدافها السياسية، وبناء قوة الردع اللازمة، وتنمية التبادل التجاري"،والبعُد العسكري بتحقيق مطالب الدفاع من خلال بناء قوة عسكرية قادرة على تحقيق التوازن الاستراتيجي العسكري والردع الدفاعي والبعُد الاجتماعي هو إقامة العادلة الاجتماعية وتقريب الفوارق بين الطبقات وتطوير الخدمات ([84])

ويبين مما تقدم أن قانون الاتصالات قد وضع تعريفا واسعا للأمن القومي، في حين حددت محكمة القضاء الإداري بشكل واضح ما هو المقصود به، وفي نطاق أضيق كثيرا ويتصل بمجالات محددة، ونحن نميل إلى التوجه الذي تبنته محكمة القضاء الإداري في هذا الصدد، باعتبار أن الأمن القومي في مجال حرية تداول المعلومات هو استثناء على الأصل، ومن ثم

يجب أن يكون محدودا لأقصى درجة ممكنة، حتى يمكن الوقاية من الجور على القاعدة العامة التي تقضى بإتاحة المعلومات كأصل عام

المطلب الثالث

حماية أمن المعلومات فى المواثيق والمعاهدات الدولية([85])

ينص العهد الدولي للحقوق المدنية والسياسية في مادته رقم (17) على:

1- لا يجوز تعريض أي شخص، على نحوٍ تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

2- من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس". وقد صدَّقت مصر على العهد الدولي للحقوق المدنية والسياسية، حيث تم نشر قرار رئيس الجمهورية رقم 536 لسنة 1981 بالجريدة الرسمية، مع الأخذ في الاعتبار أحكام الشريعة الإسلامية.

شهدت أوروبا ، تطوير هذه الفكرة ضمن حزمة شاملة من مبادئ السلوك والممارسات المقبولة ، أهمها تأكيد الاستخدام العادل والمنصف للبيانات الشخصية ، والتدخل بالحدود الدنيا ، وتقييد وتضييق أغراض استخدام البيانات وحصر الاستخدام في غرض الجمع.

ففي ألمانيا ظهرت اول معالجة تشريعية في ميدان حماية البيانات كان عام 1970 في ولاية هيس بالمانيا) ، لكن هذه المعالجة لا تعد قانونا متكاملا لاعتبارات عديدة اولها انه ليس قانون دولة ، وقد تبعه سن اول قانون وطني (متكامل) في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم المانيا على المستوى الفدرالي عام 1977 ثم فرنسا عام 1978 وفي عام 1981 وضع مجلس أوروبا اتفاقية حماية الافراد من مخاطر المعالجة الالية للبيانات الشخصية ، ووضعت كذلك منظمة التعاون الاقتصادي والتنمية دليلا ارشاديا لحماية الخصوصية ونقل البيانات الخاصة([86]) ، والذي قرر مجموعة قواعد تحكم عمليات المعالجة الإلكترونية للبيانات ، وهذه القواعد تصف البيانات والمعلومات الشخصية على انها معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر .ثم وفي خطوة متطورة على

المستوى التشريعي الاقليمي ، بل وذات اثر عالميا ([87])، اصدر الاتحاد الأوروبي الامر التشريعي الخاص بحماية البيانات ونقلها عبر الحدود لعام 1995، الذي مثل مرحلة جديدة في اعادة تنظيم خصوصية المعلومات ادت الى اعادة وضع العديد من دول أوروبا تشريعات جديدة او تطوير تشريعاتها القائمة في هذا الحقل ، بل اثر فيما تضمنه من معايير في حقل نقل البيانات خارج الحدود لجهة في سعي العديد من دول العالم خارج نطاق اوروبا الى التواؤم مع ما قرره هذا الأمر التشريعي ، وبالعموم يمكننا القول بإيجاز ان مفهوم حماية البيانات في المواثيق المتقدمة يتطلب ان تكون البيانات الشخصية([88]) -:

1- قد تم الحصول عليها بطريق مشروع وقانوني .

2- تستخدم للغرض الأصلي المعلن والمحدد ولا تكشف لغير المصرح لهم بالاطلاع عليها

3- تتصل بالغرض المقصود من الجمع ولا تتجاوزه ومحصورة بذلك .

4- صحيحة وتخضع لعمليات التحديث والتصحيح .

5- يتوفر حق الوصول اليها مع حق الإخطار بأنشطة المعالجة او النقل وحق التصحيح والتعديل وحتى طلب الالغاء .

6- تحفظ سرية وتحمى سريتها وفق معايير امن ملائمة لحماية المعلومات ونظم المعالجة .

7- تتلف عند استنفاذ الغرض من جمعها .

وقد تناول تقرير مفوض الأمم المتحدة لحقوق الإنسان الذي نُشر في عام 2018 مسألة الحق في الخصوصية في العصر الرقمي([89])، استنادًا إلى عدة مواثيق دولية وإقليمية، من بينها العهد الدولي للحقوق المدنية والسياسية.

بناءً على ذلك. تم أنشأ مجلس حقوق الإنسان الخاص المعني بالحق في الخصوصية يوليو ٢٠١٥.

وفي العديد من القرارات، أعرب مجلس حقوق الإنسان والجمعية العامة عن مخاوفها بشأن المخاطر التي تهدد الخصوصية نتيجةً للتدابير التي تتخذها الدول من أجل فرض المراقبة أو نتيجةً للممارسات الصادرة عن قطاع الأعمال.

وخصوصية المعلومات لا تشمل فقط المعلومات المتوافرة، وإنما أيضًا البيانات الوصفية التي يمكن من خلال تحليلها أن توفر نظرة عن سلوك الفرد وعلاقاته وتفضيلاته.

-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:

الموقعة في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠ ، ووافقت مصر على الانضمام إليها ٢٠١٤ ،وتهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

وتعد هذه الاتفاقية من أهم الاتفاقيات العربية التي أبرمت في مجال مكافحة الجريمة التقنية بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، مثل الاعتداء على سلامة البيانات، وجرائم إساءة استخدام وسائل تقنية المعلوماتية، والتزوير والاحتيال والإباحية والاعتداء على حرمة الحياة الخاصة([90])، والجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات مثل نشر أفكار جماعات إرهابية والدعوة لها، وتمويل العمليات الإرهابية ونشر طرق صناعة المتفجرات، وأيضا ما يتعلق بالجريمة المنظمة مثل غسل الأموال والترويج للمخدرات والاتجار بالبشر والأعضاء البشرية والأسلحة.

المطلب الرابع

القواعد الدولية لحماية امن المعلومات

الحق في الخصوصية احد حقوق الانسان الاساسية الذى اعترف بها الاعلان العالمي لحقوق الانسان والعهد الدولي للحقوق المدنية والسياسية واتفاقية حقوق الانسان الاوروبية والاتفاقية الأمريكية لحقوق الإنسان وغيرها.([91])

وللخصوصية وفق تطورها التاريخي ثلاث محطات رئيسة:

الاولى :- الاعتراف بالخصوصية كحق لحماية الافراد من مظاهر الاعتداء المادي على حياتهم وممتلكاتهم، وهي ما تعرف بالخصوصية المادية.

والثانية :- انطواء الخصوصية على حماية القيم والعناصر المعنوية للشخص، وهي ما عرف بالخصوصية المعنوية.

والثالثة الخصوصية([92]) كحق عام يمتد نطاقه لحماية الشخص من كافة اوجه الاعتداءات والتدخل في حياته ايا كان مظهرها او طبيعتها، وفي نطاق المعنى الاخير، ولد مفهوم جديد للخصوصية ارتبط باثر التقنية على الحياة الخاصة، تمثل بخصوصية المعلومات او حق الافراد في السيطرة على المعلومات والبيانات الخاصة في مواجهة تحديات العصر الرقمي .

ويمكننا القول ان كافة دول العالم على وجه التقريب أقرت بشكل او بآخر بالحق في الخصوصية في واحد او اكثر من مظاهره، وهذا لا يعني توفر حماية كافية، او شمولية في الحماية لدى كافة الدول، وفي الوقت الذي قد نجد فيه حماية الخصوصية بمفهومها المادي اكثر شيوعا واتساعا، تضيق حماية خصوصية المعلومات، وفي ذات الوقت نجدها الشغل الشاغل في الوقت الحاضر للمؤسسات التشريعية ومؤسسات القرار في العديد من دول العالم([93]).

وكانت أول معالجة تشريعية في ولاية هيس بالمانيا لكن هذه المعالجة لا تعد قانونا متكاملا لاعتبارات عديدة اولها انه ليس قانون دولة، وقد تبعه سن اول قانون وطني (متكامل) في السويد عام 1973 ثم الولايات المتحدة عام 1974 ثم المانيا على المستوى الفدرالي عام 1977 ثم فرنسا عام 1978 .

وقد شهدت الستينات انطلاق الاهتمام بحماية الخصوصية من مخاطر التكنولوجيات الحديثة([94])، لينطلق معه مفهوم حماية البيانات الخاصة من مخاطر التقنية، ومنذ مطلع

السبعينات بدأت دول العالم تتبنى قوانين حماية الخصوصية اما عن طريق القوانين الشمولية التي تعترف بالحق وتقر المبادئ الأساسية وتقدم الاطار القانوني الموضوعي والإجرائي لحماية خصوصية المعلومات او حماية البيانات التي تتصل بالافراد وحياتهم الخاصة (البيانات الشخصية)، او عن طريق حزمة قوانين تتعلق بالبيانات في قطاعات معينة، كالبيانات الصحية او المالية او بيانات الاحوال المدنية او غيرها، الى جانب مدونات سلوك تحكم قطاعات معينة كقطاعات الصناعة او الخدمات التقنية فيما يعرف بوسيلة التنظيم القانوني الذاتي للقطاعات او السوق. وغالبية هذه القوانين ان لم تكن كلها اعتمدت في محتواها وما تضمنته على قرارات مجلس أوروبا عامي 73 و74 واتفاقية (مجلس اوروبا) الخاصة بحماية البيانات من مخاطر المعالجة الآلية لعام 1980 ،وعلى دليل منظمة التعاون الاقتصادي والتنمية ودليل الامم المتحدة اللاحق عام 1990 ،وفي تطورها وشموليتها خلال السنوات الخمس الأخيرة اعتمدت بشكل واضح على تعليمات (الامر التشريعي) للاتحاد الأوروبي لحماية البيانات عام 1995 ،وقد مثلت قواعد هذه المدونات ما يمكن تسميته الشرعية الدولية لحماية البيانات أو دستور خصوصية المعلومات.

وهي تسمية نطلقها في هذه المرحلة من تطور موضوع خصوصية المعلومات لما لمسناه من اثر حقيقي لها في صياغة النظام القانوني لحماية البيانات والخصوصية في العصر الرقمي .

كذلك اصدر الاتحاد الاوروبي في عام 1995 دليلا شاملا – ملزما لدول الاتحاد الاوروبي ، ولهذا نطلق عليه الأمر التشريعي يتعلق بحماية خصوصية المعلومات وتنظيم نقل المعلومات خارج الحدود، وقد اقر من قبل البرلمان الاوروبي ومجلس اوروبا معا، وتبعه عام 1997 دليل اخر لتنظيم معالجة البيانات الشخصية في قطاع الاتصالات، وهذا الجهد الجديد – مضافا اليه استمرار الجهود من قبل اطر الامم المتحدة ومؤسسات اوروبا الموحدة ومنظمة التعاون الاقتصادي والتنمية عبر اصدار ادلة متعددة تعالج مختلف طوائف البيانات وحمايتها في البيئة الرقمية .

وتميز الامر التشريعي للاتحاد الاوروبي لعام 1995 بالزام الدول الاوروبية بإدماجه ضمن تشريعاتها في فترة أقصاها نهاية أكتوبر 1998 ،وهو ما ادى الى موجة تشريعية جديدة وموجة تعديل التدابير التشريعية القائمة في مختلف دول اوروبا، وتحديدا الدول الخمسة عشر الأعضاء في الاتحاد، واثر ذلك على عشرات دول العالم من خارج اوروبا التي وجدت في هذه التجربة الناضجة لحماية البيانات الشخصية([95]) هاديا لها ونموذجا متقدما امكنها الاعتماد عليه لاقرار تشريعات حماية البيانات الشخصية او تشريعات الخصوصية الشمولية في دولها .

وساهم في ذلك ان الامر التشريعي الأوروبي لعام 1995 نظم حماية البيانات الشخصية وبنفس الوقت الحق في نقل البيانات خارج الحدود وهو جزء من مسائل الحق في الوصول للمعلومات ([96]) فقد قامت بريطانيا عام 1998 بتسمية جهة الرقابة على حماية البيانات الشخصية بمفوض حماية البيانات في اعقاب قانون حماية البيانات البريطاني لعام 1998) .

اذا يمكننا القول ان خصوصية المعلومات هي حماية البيانات ، لكن الخصوصية ليست هي حماية البيانات، فالاخيرة شيء من الخصوصية وتتعلق بمواجهة الاعتداءات على البيانات

الشخصية([97]) وتنظيم الحق في البيانات الشخصية وسيطرة صاحبها عليها، في حين ان الخصوصية على اطلاقها ، تنطوي على خصوصية البيانات، وخصوصية الاتصالات في مواجهة انشطة الرقابة والتجسس، وخصوصية المكان وحرمته في مواجهة انشطة الاعتداء المادية، وهي مسائل حرمة المسكن وحرمة الشخص من التفتيش غير القانوني، وايضا خصوصية المراسلات ومن ضمنها مراسلات مادية واخرى الكترونية، وغير ذلك من اوجه الحماية ذات الطبيعة او المحتوى المادي او المعنوي ([98]).

المطلب الخامس

التعاون الدولى لحماية امن المعلومات([99])

لقد كان حرص المشرع المصري واهتمامه واضحاً في تيسير سبل التعاون الدولي في مجال مكافحة الجريمة قبل وقوعها، وتبادل المعلومات والبيانات اللازمة عنها حال وقوعها، وضبط وتسليم المجرمين الهاربين، والمساعدة في إجراء التحقيق معهم، أي تطبيق مبدأ العالمية الجنائية والإجرائية([100])، وقواعد تسليم المجرمين الهاربين في إطار الاتفاقيات والمعاهدات الدولية والإقليمية المصدق عليها فيما بينهم، وظهر ذلك بوضوح في المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات المصري التي نصت على أن "تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقاً لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة في هذا الشأن"([101])

ويعد مسلك المشرع المصري بإدراج نص خاص يتضمن الاهتمام بالتعاون الدولي وتيسيره في مجال مكافحة الجريمة المعلوماتية التقنية تفعيلاً حقيقياً لمبادئ وأهداف الاتفاقية العربية لمكافحة الجريمة المعلوماتية، الواردة في المادة الأولي منها والتي نصت على أن تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها([102]).

والى جانب هذا الهدف الرئيسي والهام فقد تضمنت الاتفاقية العربية العديد من النصوص المتعلق بتفعيل التعاون الدولي في مجال مكافحة هذه الطائفة من الجرائم المستحدثة، بدءا من المادة ٣٠ وحتى المادة ٤٣ من الاتفاقية.

الاتفاقيات الدولية المتعلقة بالحد من حروب الفضاء الإلكتروني

صدر عن مؤتمر الأمم المتحدة ما عرف بإعلان فيينا بشأن الجريمة والعدالة"([103])، وجاء النص في الفقرة الثامنة عشرة منه على" الجرائم الحاسوبية"، حيث نصت على((نقرر صوغ توصيات سياسية ذات توجه عملي بشأن منع ومكافحة الجريمة المتعلقة بالحواسيب، وندعو

لجنة منع الجريمة والعدالة الجنائية إلي الاضطلاع بعمل في هذا الشأن، آخذة في الاعتبار الأعمال الجارية في محافل أخرى .

إلا إن مثل هذه التوصيات ظلت في إطار السعي لبلورة منظومة تشريعية تنطلق من التعامل مع هجمات الفضاء الإلكتروني باعتبارها مسألة تتعلق بجرائم ذات طابع جنائي بالدرجة الأولى وليست باعتبارها نوعا وشكلا جديدا من المواجهات الدولية.

اعتمد البرلمان الأوروبي" الاتفاقية الأوروبية بشأن الجريمة السيبرانية، قد أنشأت لجنة خبراء للتعامل مع مشكلة الجريمة في الفضاء الإلكتروني، عملت على إعداد مشروع الاتفاقية التي اعتمدها البرلمان، ووصل عدد الدول المصادقة على الاتفاقية إلى ثلاثين دولة.

هدفت الاتفاقية الأوروبية إلى توحيد التشريعات الجنائية المتعلقة بالجرائم الإلكترونية، وتوفير الإجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيا بواسطة الحواسيب . كما هدفت إلى تأسيس نظام سريع وفعال للتنسيق والتعاون الدولي فيما يتعلق بالتصدي لجرائم وهجمات الفضاء الإلكتروني، بما في ذلك إجراءات المساعدة المتبادلة في جمع حركة المعلومات واعتراضها، والحفاظ على البيانات المخزنة على أجهزة الحاسوب والإفصاح عن حركة هذه البيانات، وجمع المعلومات عن حركة البيانات وعن إمكان وجود تد خل في محتواها، والتعاون في تسليم المجرمين([104]).

ووفقا للاتفاقية فإن مصطلح" جرائم الإنترنت "يتناول النشاطات غير المشروعة المرتبطة بأجهزة الحاسوب وباستخدام شبكة الإنترنت .

وقد صنفت جرائم الإنترنت إلى أربعة أنواع هي :أعمال القرصنة والجرائم ضد سلامة المعلومات وخصوصيتها، وجرائم التدخل بأنظمة الحاسوب وبرامجه، والجرائم التي تتعلق بالعلامات التجارية والملكية الفكر ية، والتجسس على البيانات والمعلومات .

وقد أوجبت الاتفاقية على الدول الأعضاء اتخاذ تدابير تشريعية للنص على المسؤولية عن الشروع والتدخل والتحريض في ارتكاب هذه الجرائم، وذلك بغرض وجود رادع عام لما لهذه الجرائم([105]) من تأثير بالغ على اقتصاديات الدول.

صدر عن الأمم المتحدة القرار بشأن مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات .وتضمن هذا القرار دعوة الدول الأعضاء، إلى وضع التشريعات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات .

صدر القرار58 حول موضوع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي .وانطلق من التأكيد على ملاحظة تحقق تقدم كبير في تطوير وتطبيق أحدث تكنولوجيات المعلومات ووسائل الاتصالات السلكية واللاسلكية، ومن ثم التأكيد على أن تكنولوجيات المعلومات والاتصالات ذات الاستخدام المزدوج يمكن استخدامها لأغراض مشروعة وخبيثة على حد سواء.

وشددَ القرار على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، مع التأكيد في هذا السياق على الدور الذي يمكن أن تؤديه الأمم المتحدة وغيرها من المنظمات الدولية والإقليمية وشدد على أن من مصلحة جميع الدول تشجيع استخدام تكنولوجيات المعلومات والاتصالات في الأغراض السلمية، بهدف صوغ مستقبل مشترك للبشرية جمعاء في الفضاء الإلكتروني، وأن للدول أيضا مصلحة في منع نشوب النزاعات الناشئة عن استخدام تكنولوجيا المعلومات والاتصالات.

وبعد ذلك صدر تقرير عن مجموعة من الخبراء - شكلت من قبل مجلس الأمم المتحدة - وأقرته مجموعة العشرين، يقضي بوضع معايير للحد من المواجهات في الفضاء الإلكتروني([106]) .

وقد تضمن هذا التقرير معايير لمعالجة سلامة وأمن البيانات، وكان هناك اتفاق عام على تدابير بناء الثقة، ووضع قواعد لقضايا من قبيل الجريمة وحرب المعلوماتة.

وخلال سنوات ارتفع عدد الدول الأعضاء المشاركة في فريق الخبراء الحكوميين ووصل إلى خمسة وعشرين دولة، وأصبحت القضايا موضوع النقاش أكثر دقة .ولكن مع تنامي الأعداد ازدادت صعوبة التوصل إلى اتفاق إلا إن الفريق فشل في إصدار تقرير بتوافق أوسع .وكان السبب أن الولايات المتحدة والدول الغربي ة المقاربة لوجهة نظرها، ضغطت من أجل مزيد من التوضيح لكون القوانين الدولية المتعلقة بالصراع المسلح، بما في ذلك حق الدفاع عن النفس في الفضاء الإلكتروني، وهو ما تعذر تحقيق التوافق من قبل الخبراء بخصوصه.

وقد ظلت عملية البلورة متعثرة خلال السنوات اللاحقة حتى يومنا هذا، وذلك لكونها تتطلب مناخ سياسي دولي إيجابي وتفاهمات وتوافقات دولية موسعة وهو ما لم يكن متوفرا خلال السنوات الأخيرة، مع زيادة حدة الخلافات والتنافس الدولي وبخا صة بين كل من روسيا والصين والولايات المتحدة.

المطلب السادس

التشريعات الدولية في مجال الانترنت

يعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني وقد أسّست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت.

وأبرز المجموعات والمنظمات الدولية التي عملت في موضوع امن المعلومات نذكر([107]):

أ.مجموعة الدول الثماني G8

ب. الأمم المتحدة ومنظماتها

ج. الاتحاد الدولي للاتصالات

د. مجلس أوروبا

أ. مجموعة الدول الثماني: G8

إعتمد وزراء العدل والداخلية التابعين لبلدان الـ G8 في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية: عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر، تدريب الموظّفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

بالإضافة الى ذلك، دعت دول الـ G8 إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد إتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن تثمير الدراسات العديدة التي وضعتها دول الـ G8 ومن بينها: مبادىء وخطة العمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر (1997) ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول (1999) وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية (2002) ومبادئ توافر البيانات الأساسية لحماية السلامة العامة (2002) وإعلان بيان دول G8 على نظم حماية المعلومات (2002).

ومن توصيات الـ G8 بالنسبة لجرائم التكنولوجيا المتقدمة والجرائم ذات الصلة بالكمبيوتر موجودة في إطار الباب D من المعاهدة وتتلخص بما يلي:

- يتعيّن على الدول أن تُجرّم الانتهاكات على حقوق الغير الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي في ما يتعلّق بمكافحة هذه الانتهاكات.

- ينبغي للدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:

• التعاون مع القطاع الصناعي لضمان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الالكترونية للهجمات.

• سن قوانين وتدابير أخرى وتنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير والقرصنة.

• تحديد المشاكل المحتملة ومعالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.

• نشر الوعي العام في ما يتعلق بموضوع الجريمة ذات التقنية العالية.

- يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق والادعاء العام، من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيا الكمبيوتر لارتكاب جرائمهم. ويتوجّب على الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.

- ينبغي تحسين التواصل بين الموظفين المكلّفين تطبيق القوانين في مختلف الدول، بما في ذلك تبادل الخبرات في معالجة هذه المشاكل.

- يتوجب على الدول الحفاظ على التوازن المناسب بين حماية الحق في الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.

- على الدول تشجيع وضع القوانين وتنفيذ تدابير لتوفير حماية فعالة للأطفال من جميع أشكال الاستغلال الجنسي على الإنترنت.

- على الدول أن تتعاون من أجل التطوير المستمر للموارد والتقنيات والتدريب للمساعدة في تطبيق القانون ومكافحة الاستغلال الجنسي للأطفال عبر الإنترنت. كما ينبغي العمل مع مقدمي خدمة الإنترنت والمنظمات غير الحكومية لتطوير الطرق التي يمكن أن تساعد هذه المنظمات من أجل تطبيق قوانين مكافحة الاستغلال الجنسي للأطفال على شبكة الإنترنت.

وأخيرًا، على الدول أن تشجّع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن، وكذلك التقييم المستمر لبرامج المكافحة والوسائل القانونية المتبعة([108]).

ب. قرارات الجمعية العامة للأمم المتحدة

تعمل الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية (الانترنت). وتشارك وكالات الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدد من القضايا، بما في ذلك وضع معايير توفير الحماية لشبكات الانترنت. أما أبرز قرارات الجمعية العامة للامم المتحدة في هذا المجال فهي:

- القرار 121/45 العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

- القرارات 70/53 في 4 ديسمبر 1998، و49/54 في ديسمبر 1999، 28/55 في 20 نوفمبر 2000 و19/56 في 29نوفمبر 2001 و53/57 في 22 نوفمبر 2002 و32/58 في 18 ديسمبر 2003 حول موضوع «التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي».

- القرارات 63/55 في ديسمبر 2000، و121/56 في 19 ديسمبر 2001 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار 239/57 في 20 ديسمبر 2002 بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

- قرارات الجمعية العامة 239/57 في 31 يناير 2003 و199/58 في 30 يناير 2004 بشأن «إنشاء ثقافة عالمية للأمن السيبراني»، والذي يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني([109])

من ناحية أخرى، هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل:

• القرار CCPCJ 16/2/2007 من أبريل 2007 «المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال» (الفقرات 7، 16).

• قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ 26 يوليو 2007 بعنوان «التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية» (E/2007/30 وE/2007/SR.45).

• قرار المجلس الاقتصادي والاجتماعي 26/2004 بتاريخ 21 يوليو 2004 بعنوان «التعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة».

• الفقرة 18 من «إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين»، التي أقرتها الجمعية العامة في القرار 59/55 المؤرخ 4 ديسمبر 2000 والفقرة 36 المرفقة بقرار الجمعية العامة 261/56 المؤرخ 31 يناير 2002 حول: «خطط العمل لتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين».

• الفقرتان 15 و16 من إعلان بانكوك بشأن «أوجه التآزر والتعاون: التحالفات الاستراتيجية في مجال منع الجريمة وتحقيق العدالة الجنائية»، الذي أقرّه قرار الجمعية العامة 177/60 بتاريخ 16 ديسمبر 2005.

• توصيات مؤتمر ورشة العمل على([110]) «التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر»، الذي عقد في بانكوك في 22 أبريل 2005 كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية. الفقرة 2 من قرار الجمعية العامة 177/60 التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

• قرار لجنة مكافحة المخدرات 5/48 حول «تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات».

• الفقرة 17 من قرار الجمعية العامة 178/60 المؤرخ 16 ديسمبر 2005 بخصوص «التعاون الدولي لمكافحة مشكلة المخدرات العالمية».

• قرار لجنة مكافحة المخدرات 8/43 في 15 مارس 2000 عبر الإنترنت.

• قرار المجلس الاقتصادي والاجتماعي 42/2004 بشأن «بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت».

• مختلف توصيات الهيئات الفرعية التابعة للجنة مكافحة المخدرات واللجنة الفرعية المعنية بالاتجار غير المشروع بالمخدرات والمسائل المتعلقة بالشرقين الأدنى والأوسط.

• التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت العام 2005 وتوصيات للحد من انتشار المبيعات غير المشروعة من المواد الخاضعة للرقابة ولا سيما المستحضرات الصيدلانية، عبر الإنترنت.

تدعو الجمعية العامة في قراراتها المختلفة - التي غالبًا ما تكون مماثلة لقرارات الاتحاد الدولي للاتصالات - الدول الأعضاء، عند وضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ في الاعتبار أعمال لجنة منع الجريمة ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية.

ج. الاتحاد الدولي للاتصالات

يوفّر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجيا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة. ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا «لتعزيز الأمن السيبراني العالمي يتكوّن من سبعة أهداف رئيسة، والأهداف السبعة هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الانترنت.

- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.

- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.

- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها([111]).

د. إتفاقية المجلس الأوروبي بشأن جرائم الإنترنت

إعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976. وفي العام 1996، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة

السيبرانية. عملت اللجنة بين العامين 1997 و2000 على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أبريل 2001. وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010.

إن إتفاقية جرائم الانترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى.

تهدف الاتفاقية إلى:

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر([112]).

- تعيين نظام سريع وفعال للتعاون الدولي.

- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

- تتضمن أيضًا الاتفاقية المبادئ العامة المتعلّقة بالتعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.

- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.

- الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

نتائج البحث

من خلال هذه الدراسة رأينا التعاون الدولى لمكافحة جرائم المعلومات وكيف تصدت العديد من دول العالم لهذا الخطر التقني، وحرصت على تطوير نظم المكافحة التشريعية لديها، بإدخال نصوص تشريعية تتوافق مع ظاهرة الإجرام التقني الحديثة، ، لتكفل لها الحماية اللازمة من مثل هذه الاعتداءات والمخاطر، ونشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها وبيان وسائل وطرق الوقاية منها.

ورأينا أيضاً كيف كان المشرع المصري متطوراً وموفقاً إلى حد كبير في إصدار العديد من التشريعات والنصوص، ووضع الحلول التشريعية اللازمة، أو المناسبة لمكافحة هذه الجرائم الناشئة عن استخدام وسائل التقنية المعلوماتية، أو الحد منها ،وخروجه عن نطاق المكافحة التقليدية التي أصبحت لا تتناسب وهذا الإجرام التقني الحديث، نظراً لما تتميز به جرائم تقنية المعلومات من السهولة في ارتكابها، والقدرة على إخفاء أدلتها وآثارها، وقدرة الجناة على الهرب، وشعورهم بأنهم خارج حدود الرقابة والسيطرة القانونية والأمنية.

وتعرفنا من خلال هذا البحث على القانون المصري رقم ١٧٥ لسنة ٢٠١٨ ، وأهم الجرائم التقنية وحدود العقوبات المقررة لها، كما تعرفنا على أهم الاحكام الاجرائية المنظمة لمكافحة هذه الظاهرة الاجرامية التقنية ، وضوابط التعاون الدولي في مكافحتها والحد منها.

التوصيات:

توصلنا من خلال هذه الدراسة إلي مجموعة من التوصيات كان من أهمها:

1-للابد من وجود نصوص عقابية رادعة لمنتهكي المعلومات وسارقيها، وهو ما يهدد باستمرار الاخلال بأمن المعلومات، وهو ما ينبغي التصدي له بنصوص رادعة.

2- ضرورة مواكبة التطورات الحاصلة في بيئة تكنولوجيا المعلومات وتطويرها .

3- الاهتمام بالمعايير العالمية الخاصة بأمن المعلومات والتى من اهمها معيار الايزو 27001 الذى يعتبر الدليل والمرشد في هذا المجال

4- توفير احدث الانظمة وبرمجيات الحماية وتطوير قواعد البيانات ليسهل من توفير الحماية لها من اى اعتداء

5- ضرورة تسليح القاضي الجنائي بتقنية وعلوم الحاسب الآلي لمواكبة المناقشة العلمية للاجرام التقنى وذلك عن طريق عقد دورات تدريبية لأعضاء النيابة العامة والقضاة لتثقيفهم فنياً والإلمام بالأمور الفنية التي تعينهم على كشف الجرائم المعلوماتية التقنية والتحقيق فيها ومعرفة عناصرها وأسرارها..

6- إضافة مقرر دراسي لطلاب كليات الحقوق تتضمن معلومات عن الحاسب الآلي وتقنياته و طرق الاثبات و التحقيق في القضايا المتعلقه بالحاسب الالي

7- نوصى المشرع إعادة النظر في قانون مكافحة جرائم تقنية المعلومات والنص صراحة على بعض الجرائم التقليدية التي تطورت وأصبحت ترتكب بواسطة وسائل التقنية الحديثة مثل النصب، والتزوير، والقرصنة، والسرقة، وانتحال الصفة، والتحرش والإرهاب الالكتروني، وانتهاك الخصوصية والإساءة للغير، والتجسس...الخ (وإدراجها في نصوص عقابية رادعة تتناسب وخطورتها.

8- الاستثمار في الجانب البشرى اكثر منه في الجانب المادى واختيار احسن الكفاءات للتعامل مع انظمة المعلومات وإعداد وتنمية الكوادر الفنية المتخصصة للاستعانة بهم في معاونة رجال الأمن والقضاء في كشف الجريمة والتحقيق فيها.

9 - ابرام المزيد من الاتفاقيات والمعاهدات المتعلقة بهذا الشأن لتوحيد الجهود التشريعية في مجال المواجهة الدولية لهذا الخطر التقني والتعاون الفعال في تطبيق قواعد تسليم المجرمين الهاربين مع الأخذ في الاعتبار الاتفاقيات والمعاهدات الدولية الأوروبية.

10 - تشجيع البحث والدراسة في هذا المجال التقني وتوفير سبل الدعم والمساعدة للباحثين والمتخصصين.

11 – التوعية الاعلامية بصور الجرائم التقنية والنصوص العقابية المقررة عليها، والأصول العلمية واجبة الإتباع لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الرقمية التقنية، وكافة القرارات والتعليمات التنظيمية الصادرة في هذا الشأن.

ملحق

لنماذج قوانين حماية المعلومات حول العالم

تونس

- قانون ٦٣ لسنة ٢٠٠٤ بشأن حماية البيانات الشخصية.

- المواد ٥٦ و ٦١ و ٧٥ من قانون مكافحة الإرهاب وجرائم غسيل الأموال، تعالج مسألة الشخص المعنى بالبيانات وحالات السماح باستخدام البيانات الشخصية.

- في عام ٢٠١٨ تم تقديم مسودة لقانون جديد لحماية البيانات الشخصية يتوافق مع اللائحة الأوروبية لحماية البيانات (GDPR) إلى البرلمان التونسي.

البحرين

قانون رقم ٣٠ لسنة ٢٠١٨ لحماية البيانات الشخصيةPDPL

دخل حيز النفاذ في أغسطس ٢٠١٩

المغرب

قانون رقم ٠٩ ـ ٠٨ لسنة ٢٠٠٩ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية، مع المرسوم التنفيذي رقم ٢ ـ٠٩ ـ ١٦٥ لسنة ٢٠٠٩ ، يمثلان معًا قانون حماية البيانات في المغرب.

قطر

قانون رقم ١٣ لسنة ٢٠١٦ دخل القانون حيز النفاذ في عام ٢٠١٧ إلا أن لوائحه التنفيذية لم تصدر بعد، ومن المتوقع صدورها خلال العام الجاري 2022

تركيا

- قانون رقم ٦٦٩٨ لسنة ٢٠١٦ ، القائم على التوجيه الأوروبي رقم95 / EC/46 اللائحة المتعلقة بمحو، وتدمير، وإخفاء البيانات الشخصية رقم ٣٠٢٢٤ لعام ٢٠١٧.

- لائحة إجراءات ومبادئ مجلس حماية البيانات الشخصية، رقم ٣٠٢٤٢ لسنة ٢٠١٧.

- لائحة سجل المتحكمين في البيانات، رقم ٣٠٢٨٦ لسنة ٢٠١٧.

- لائحة تنظيم هيئة حماية البيانات الشخصية، رقم ٣٠٤٠٣ لسنة ٢٠١٨.

- قرار مجلس حماية البيانات الصادر بتاريخ ٣١ يناير ٢٠١٨ ، برقم ١٠ / ٢٠١٨ ، بشأن التدابير المطلوب اتخاذها من قِبَل المتحكمين بالبيانات في معالجتهم للفئات الخاصة من البيانات الشخصية.

جنوب افريقيا

- قانون حماية المعلومات الشخصية POPIA.رقم ٤ لسنة ،٢٠١٣

سيدخل القانون حيز النفاذ بشكل كامل ف ي ٣٠ / ٦ / ٢٠٢١.

- قانون حماية البيانات، رقم ٢٢ / ١١ ، لسنة ٢٠١١.
- قانون حماية النظم المعلوماتية والشبكات، رقم ٧ /١٧ ، لسنة ٢٠١٧
- قانون رقم ٨٤٣ لسنة ٢٠١٢

القانون لم يدخل حيز النفاذ بعد، ومن المتوقع أن يُنشر بالجريدة الرسمية وينفذ خلال العام الجاري.

الحالات الثمانية للمعالجة القانونية.

-القيود على معالجة البيانات الشخصية ذات الطابع الخاص والبيانات الشخصية المتعلقة بالأطفال.
-الاحكام الخاصة بالاستثناءات.
- المتطلبات الخاصة بالتصاريح المسبقة.
-الأحكام الخاصة بإنفاذ القانون، وبالجرائم والعقوبات.
-احكام عامة متعلقة بالرسوم، وبالتدابير الانتقالية

انجولا

-قانون حماية البيانات، رقم ٢٢ / ١١ ، لسنة ٢٠١١.
-قانون حماية النظم المعلوماتية والشبكات، رقم ٧ /١٧ ، لسنة ٢٠١٧.

غانا

قانون رقم ٨٤٣ لسنة ٢٠١٢

القانون لم يدخل حيز النفاذ بعد، ومن المتوقع أن يُنشر بالجريدة الرسمية وينفذ خلال العام الجاري.

كوريا الجنوبية

قانون حماية البيانات PIPA الصار في عام 2012

اليابان

-قانون حماية البيانات، رقم ٢٢ / ١١ ، لسنة ٢٠١١.
-قانون حماية النظم المعلوماتية والشبكات، رقم ٧ /١٧ ، لسنة ٢٠١٧.

المراجع

1 -د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، 2015 ص76
2 - د /أحمد شـوقي عمر أبو خطوة -شـرح الأحكام العامة لقانون العقوبات، الجزء الأول –النظرية العامة للجريمة، دار النهضة العربية، القاهرة، .١٩٩٩ ص211
3 - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي ،رساله ماجيستير، بيروت، ط1، 2005.ص11
4 . د. هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ، القاهرة: دار النهضة العربية ، الطبعة الأولي1997ص56
5 -نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي ، مرجع سابق ص22
6 د. غنام محمد غنام, عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم إلى مؤتمر القانون والكمبيوتر ، كلية الشريعة والقانون ، جامعة الإمارات العربية المتحدة ، مايو 2000 ص87
7 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص97
8-جبور، منى الأشـقر (الأمن السـيبراني: التحديات ومسـتلزمات المواجهة، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، اللقاء السنوي في امن وسلامة الفضاء السيبراني2012)ص22.
9 د /جميل عبد الباقي –الانترنت والقانون الجنائي –الأحكام الموضـوعية للجرائم المتعلقة بالانترنت، دار النهضة العربية، ١٩٩٩ص45
10 . د. هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ،مرجع سابق ص67
11 - د. هلالي محمد عبد اللاه أحمد ، حجية المخرجات الالكترونية في المواد الجنائية بدون دار نشر 1999. ص87
12 - د /جميـل عبـد البـاقي –الانترنـت والقـانون الجنـائي –الأحكـام الموضـــوعيـة للجرائم المتعلقـة بالانترنت،مرجع سابق ص66
13 جبور، منى الأشقر (الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص28
14 - د. غنام محمد غنام, عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق ص123
15 - د. أحمد ضياء الدين محمد خليل ، مشروعية الدليل في المواد الجنائية كلية الحقوق ، جامعة عين شمس سنة 1984-ص201
16 - د. أحمد عوض بلال ، التطبيقات المعاصـــرة للنظام الإتهامي في القانون الأنجلو أمريكي ، القاهرة: دار النهضة العربية.2010 ص 87
17 هشـــام محمد فريد رســـتم ، رســـاله دكتوراه بعنون ،قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط 1992 ،ص156
18 - د.آمال عبد الرحيم عثمان ، الخبرة في المسائل القانونية رسالة دكتوراة جامعة القاهرة:.ص176
19 - . د. هلالي محمد عبد اللاه أحمد ، حجية المخرجات الالكترونية في المواد الجنائية، مرجع ســـابق ص 102
20 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص111
21 د. غنام محمد غنام, عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق 199
22 - د /أسامة عبد الله فايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات،مرجع سابق 298
23 - د /عمر محمد أبو بكر يونس –الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضـوعية والجوانب الإجرائية، رسالة دكتوراه، جامعة عين .شمس، دار النهضة العربية، القاهرة،2009 ، ص 211
24 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص166

25 -هشـام محمد فريد رسـتم ، رسـاله دكتوراه بعنون ،قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، أسيوط 1992 ،ص189
26 - حجـازي، عبـد الفتـاح بيومي (2007 م) مبـادئ الإجراءات الجنـائيـة في جرائم الكمبيوتر والإنترنـت، مرجع سابق ص6ص71
27 - الدكتور رزق سعد علي ، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة دراسة مقارنة ، دار الفكر العربى ، الامارات العربية المتحدة 2019، ص 66
28 - د /محمد سـامي الشـوا –ثورة المعلومات وانعكاسـاتها على قانون العقوبات، .دار النهضـة العربية، القاهرة، 1998،ص56
29 -- د. سامي الملا ، جرائم التكنولوجيا المعاصره ، رسالة دكتوراه ، مرجع سابق ص 165
30 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان ، 2020،ص18
31 - .غنام محمد غنام, عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق ص 146
32 - سـراج عبود مفهوم جرائم المعلوماتية، واقع وآفاق، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلومـاتيـة الـذي نظمتـه الجـامعـة الأردنيـة واتحـاد المحـامين العرب خلال الفترةمن عـام 2013،ص 65
33 - جبور، منى الأشقر (الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص128
34 - هدى حامد قشقوش ،جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة 2017 ، ص 93
35 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص33
36 - الدكتور رزق سعد علي ، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة دراسة مقارنة ، مرجع سابق ص 71
37 - د /أسامة عبد الله فايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات- مرجع سابق 240
38 - محمود أحمد، جرائم الحاسوب وأبعادها الدولية،رسالة ماجيستير، جامعة عين شمس ، 2005، ص232
39 -- الدكتور رزق سعد علي ، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة دراسة مقارنة ، مرجع سابق ص 101
40 - هدى حامد قشقوش ،جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق ص 121
41 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص37
42 - سراج عبود مفهوم جرائم المعلوماتية، واقع وآفاق، بحث مقدم إلى المؤتمر الإقليمي الأول لمكافحة جرائم المعلوماتية ،مرجع سابق ص 79
43 -- الدكتور رزق سعد علي ، انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة دراسة مقارنة ، مرجع سابق ص 121
44 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص56
45 - منير محمد الجنيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، ط1 ، 2016 ص 125
46 - هدى حامد قشقوش ،جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق ص 168
47 - للدكتور عائض المرى ، امن المعلومات ماهيتها وعناصرها واستراتجيتها – دار النور للنشر والتوزيع 2017،ص34
48 - جبور، منى الأشقر الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص37

49 - د. سامي الملا ، جرائم التكنولوجيا المعاصره ، رسالة دكتوراه ، جامعة القاهرة ، 1999ص89
50 - د /جميل عبد الباقي –الانترنت والقانون الجنائي –الأحكام الموضوعية للجرائم المتعلقة بالانترنت،مرجع سابق ص89
51 -- ابراهيم سامى و محمد اسحاق ، أمن المعلومات والانترنت ، مكتبة الاقصى2015 ص22
52 -52 - للدكتور عائض المرى ، امن المعلومات ماهيتها وعناصرها واستراتجيتها – دار النور للنشر والتوزيع 2017،ص77
53 -نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي ، مرجع سابق ص76
54 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص70
55 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص123
56 - جبور، منى الأشقر (الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص67
57- للدكتور عائض المرى ، امن المعلومات ماهيتها وعناصرها واستراتجيتها – دار النور للنشر والتوزيع 2017،ص83
58 - د. محمد فهمي طلبة ، فيروسات الحاسب وأمن البيانات ، القاهرة ، مطابع الكتاب المصري الحديث سنة ، 1992، ص11.
59 هلالي عبد اللاه أحمد ، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي دراسة مقارنة ،مرجع سابق ص96
60 - جبور، منى الأشقر (الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص80
61- ابراهيم سامى و محمد اسحاق ، أمن المعلومات والانترنت ،مرجع سابق ص56
62 - د. سامي الملا ، جرائم التكنولوجيا المعاصره ، رسالة دكتوراه ، مرجع سابق ص 103
63 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص160
64 - د /جميل عبد الباقي –الانترنت والقانون الجنائي –الأحكام الموضوعية للجرائم المتعلقة بالانترنت،مرجع سابق ص101
65 - نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي ، مرجع سابق ص88
66 - جبور، منى الأشقر (الأمن السيبراني: التحديات ومستلزمات المواجهة، مرجع سابق ،ص120
67 د. غنام محمد غنام, عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق ص 133
68 -د /أحمد شوقي عمر أبو خطوة -شرح الأحكام العامة لقانون العقوبات، الجزء الأول –النظرية العامة للجريمة، ، مرجع سابق، ص276
69 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص176
70 - د /أسامة عبد الله فايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات- .دراسة مقارنة، دار النهضة العربية، الطبعة الثانية، ١٩٩ص99
71 - (م 309 مكرر عقوبات)
72 - د /أحمد شوقي عمر أبو خطوة -شرح الأحكام العامة لقانون العقوبات، الجزء الأول –النظرية العامة للجريمة، مرجع سابق ص 301
73 - الماده (154) قانون العقوبات
74 - المادة 193 (ب) من قانون العقوبات المصرى
75 - د/ محمد عبد اللطيف عبد العال ، قانون العقوبات المصرى (القسم العام) ، دار الشروق للطباعة والنشر والتوزيع ، القاهرة 2009 ص134
76 - محمود أحمد، جرائم الحاسوب وأبعادها الدولية،مرجع سابق، ص298
77 -د/ شريف كامل ، جرائم النشر ، النهضة العربية ، القاهرة 2008 ص211
78 -د/ محمود نجيب حسنى ، شرح ثانون العقوبات ، القسم الخاص ، النهضة العربية 1981ص641

79 - د. مأمون محمد ســـلامة ، قانون الإجراءات الجنائية معلقاً عليه بالفقة والقضـــاء ، القاهرة ، دار الفكر العربي ، سنة 1981 ، ص 732
80 -د/ عمر سالم ،قانون الاجراءات الجنائية ، النهضة العربية ، القاهرة 2016
81 - د طارق سرور – جرائم النشر والإعلام – الكتاب الأول الأحكام الموضوعية – دار النهضة العربية 2008ص 820
82 -- محمد أحمد عبد الله ، الحماية القانونية لحقوق الانســـان فى ضـــوء أحكام القانون الدولى والشـــريعة الاسلامية ، المكتب الجامعى الحديث ، الاسكندرية 2007ص125
83 - على الصاوى ، الأمن القومي العربي (القاهرة: الهيئة المصرية العامة للكتاب)، 1989. ص 29.
84 -حكم محكمة القضاء الإداري – الدعوى رقم 21855 لسنة 65 ق – جلسة2011/5/28/
85 -د /جورج لبكي – المعاهدات الدولية للانترنت – حقائق وتحديات، مجلة الدفاع الوطني، بحث منشـور عبر الانترنت على موقع (http://www.lebarmy.gov.lb)
86 - د /أسامة عبد الله فايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات- مرجع سابق ص107
87 د. أحمد عوض بلال ، التطبيقات المعاصرة للنظام الإتهامي في القانون الأنجلو أمريكي ،مرجع سابق،ص 99
88 - حجـازي، عبـد الفتـاح بيومي (2007 م) مبـادئ الإجراءات الجنـائيـة في جرائم الكمبيوتر والإنترنـت، القاهرة: دار الكتب القانونية ص65
89 - مجلس حقوق الإنسـان، "الخصـوصـية في العصـر الرقمي"، أغسـطس 2018، تاريخ آخر زيارة في سبتمبر 2021، الرابطhttps://undocs.org/ar/A/HRC/39/29 :
90 - د /أسامة عبد الله فايد - الحماية الجنائية للحياة الخاصة وبنوك المعلومات- .دراسة مقارنة، مرجع سابق ص221
91- http://mawdoo3.com
92 -د/ جابر محجوب، الحق فى الحياه الخاصة، دار النهضة العربية ، القاهرة 2006 ص254
93 - د/ أنور رسلان، الحقوق والحريات العامة ، النهضة العربية ، القاهرة 2006ص120
94 - هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق ص 180
95- https://www.seu.edu.sa/sites/jisr/Pages/OneArticle.aspx
96- http://en.wikipedia.org/wiki/Internet_privacy
97 -- د/ أنور رسلان ، الحقوق والحريات العامة ، مرجع سابق ص136
98 - ســـوريـــة ديش، "أنواع الجرائم الإلكترونية وإجراءات مكافحتها"، بحث مقدم الى المركز الديمقراطي العربي،2018 ص 111
99 -د /مروي السيد السيد الحصـاوي –مبدأ العالمية في القانون الجنائي -رسـالة - دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠17ص234
100 - د. سامي الملا ، جرائم التكنولوجيا المعاصره ، رسالة دكتوراه ، مرجع سابق ص 205
101 - د /سامي على حامد عياد –الجريمة المعلوماتية وإجرام الانترنت، مرجع سابق ص186
102 - د /مروي السيد السيد الحصـاوي –مبدأ العالمية في القانون الجنائي -رسـالة .دكتوراه، كلية الحقوق – جامعة المنصورة، ٢٠١٩ ص87
103 - علي ابراهيم العناني، (2000)، المنظمات الدولية النظرة العامة،مرجع سابق،.ص273
104 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص89
105 - منير محمد الجنيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، مرجع سابق ، ص 186
106 - أسامة جلال الزعبي جرائم الحاسب الآلي الانترنت، دراسة تحليلية مقارنة،مرجع سابق،ص91
107 - United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org

108- O'Connell, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com

109 - ouncil of Europe Organized Crime Report 2004 available at: http://www.coe.int

110 - Arthur, C. (2011). Guardian.co.uk. available at: http://www.guardian.co.uk

111 - Schjolberg and Hubbard» ,**Harmonizing National Legal Approaches on Cybercrime** ,2005 ,«page 5. available at: http://www.itu.int

112 - Tinker, T., Mc Laughlin, G & ,.Dumlao, M. (2009-2010» ,(**Crisis Communication and Response** ,«Retrieved April 4, 2011, from Disaster Resource Guide:, available at: http://www.disaster-resource.com