جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها

كلية الشريعة والقانون بالقاهرة

جامعة الأزهر

العدد الأربعون

أكتوبر ٢٠٢٢م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية - كلية الشريعة والقانون - القاهرة -الدراسة - شارع جوهر القائد

ت: ٢٥١٠٧٦٨٧

فاكس: ٢٥١٠٧٧٣٨

http://fshariaandlaw.edu.eg

رقم الإيـــداع

١٨٠٥٣ / ٢٠٢٢

الترقيم الدولي للطباعة

ISSN: 2812–4774

الترقيم الدولي الإلكتروني:

ISSN: 2812–5282

الحماية الجنائية الموضوعية للتحول الرقمي

إعداد

د. عبد المطلب علي محمد بشينة

مدرس بكلية الشريعة والقانون

الجامعة الأسمرية - زليتن - ليبيا

الحماية الجنائية الموضوعية للتحول الرقمي

عبد المطلب علي محمد بشينة
قسم القانون العام، كلية الشريعة والقانون، الجامعة الأسمرية، زليتن، ليبيا.
البريد الإلكتروني: Abduoo2200@gmail.com

ملخص البحث

التحول الرقمي يفرض واقعاً جديداً يخلق فرصًا كثيرة لمراجعة القوانين وتطويرها، ولن تكون الحكومة الإلكترونية ذات جدوى دون وجود بيئة قانونية تدعم عملها، حتى تصبح المعاملات الإلكترونية، ذات صبغة قانونية، محمية بنصوص تشريعية ضد كل وسائل الاعتداء غير المشروع. وقد تناول هذا البحث الحماية الموضوعية من حيث التجريم والعقاب، ضد الأفعال غير المشروعة على كافة الوسائل التقنية الحديثة، بحيث يتم بيان الجرائم المعلوماتية وطبيعتها، ولم يقتصر على أثار التحول الرقمي على مجالات الحياة المختلفة، إنما قاد كذلك إلى تحول كبير على الجانب التشريعي للدول، لدفع السياسة الجنائية، لتطوير قواعد القوانين الجنائية. وحاولنا في هذا البحث دراسة، أسس هذا التطور في القانون الفرنسي والقانون المصري والقانون الليبي إزاء هذا التحول التقني لمؤسسات الدول، حتى نرى تعامل فعال بين البيئة الرقمية، والبيئة التشريعية تساهم في التغيير والتطوير، بحماية جنائية فعّالة. وانتهى البحث إلى عدد من التوصيات منها: ضرورة العمل على تنظيم القوانين الخاصة بمقدمي الخدمة من شركات عامة وخاصة، لحماية منظومات البيانات، وتشديد العقوبات لجرائم اختراقها، والتأكيد على ضرورة النص على تجريم الدخول غير المشروع، للجهات العامة والخاصة، غير المخولة قانوناً بتلك البيانات والمنظومات التقنية، منعاً، لإساءة استعمال السلطة، وأن يتم ذلك بإذن قضائي.

الكلمات المفتاحية: الحماية، الجنائية، التحول الرقمي، الأمن المعلوماتي، الجرائم المعلوماتية.

Substantive criminal protection of digital transformation

Abd El-Muttalib Ali Muhammad Bishina
Department of Public Law, Faculty of Sharia and Law, Asmara University, Zliten, Libya.
E-mail: Abduoo2200@gmail.com

Abstract:

Digital transformation imposes a new reality that creates many opportunities for reviewing and developing laws. E-government will not be feasible without a legal environment that supports its work, so that e-transactions, of a legal nature, become protected by legislative texts against all means of unlawful aggression. This research has dealt with the objective protection, in terms of criminalization and punishment, against unlawful acts by all modern technical means, so that information crimes are described and their nature is not limited to the effects of digital transformation on different spheres of life, but has also led to a major shift on the legislative side of States, to advance criminal policy, to develop the rules of criminal law. In this research, we tried to study the basis of this development in French, Egyptian and Libyan law in the face of this technical transformation of state institutions, so that we can see an effective interaction between the digital environment and the legislative environment that contributes to change and development, with effective criminal protection. The research concluded with a number of recommendations, including: the need to regulate the laws of public and private service providers, to protect data systems, to increase penalties for breaches of data, and to stress the need to criminalize the illegal entry of public and private entities not legally authorized by such data and technical systems, in order to prevent the abuse of power, and to do so with judicial authorization.

Keywords: Protection, Criminal, Digital Transformation, Information Security, Cyber Crime.

المقدمة

لقد أضحى التحول الرقمي ضرورة عامة، بعد ثورة المعلومات والاتصالات التي أحدثت تغييراً في المفاهيم والمصطلحات القانونية من جهة، كما أنه أدى إلى تغيير طريقة التعامل مع الأفراد وكيفية تقديم الخدمة بشكل جذري، فظهرت ما يعرف بالحكومات الإلكترونية، والشركات الرقمية، والتجارة الإلكترونية، والمدن الذكية، والتنقل الذكي، والتعلم الذكي، ودخلت أيضاً في النظام القضائي، بظهور محاكمات عبر وسائل الاتصال، واجتماعات حكومية على الصعيد الداخلي والدولي، بين الدول عبر تقنية الفيديو، وخاصة في زمان اجتياح وباء كورونا المعاصر دول العالم، فهذا النظام وفر الجهد والوقت للفرد والمؤسسة معاً، والحماية الصحية في هذا الظرف الاستثنائي، بالإضافة إلى نتيجة سابقة بأنه يسهم في خفض معدلات الفساد والقضاء على البيروقراطية.

أهمية البحث:

وللأهمية الواقع التقني الحديث، بادرت العديد من الدول للتحول الرقمي من خلال قوانين ولوائح، تلزم الجهات الحكومية والأفراد بالاستغناء عن المعاملات الورقية، مقابل منظومات رقمية في جل مؤسسات الدولة، وتتبع أهمية هذه الدراسة في مواكبتها لحالة التحول الرقمي التي بدأت بالفعل تؤتي ثمارها في بعض المجالات ذات الصلة بالمجال القانوني والقضائي بصفة عامة، ومنظومة العدالة الجنائية بصفة خاصة، وتزداد أهمية الدراسة بالنظر إلى أنها تُلمح إلى مجالات جديدة يمكن الاستعانة فيها بالتقنيات التكنولوجية الحديثة، لا سيما مع ما أكدته تجربة جائحة كورونا، وما خلفته من نتائج، كان أبرزها ضرورة العمل على إيجاد حلول غير تقليدية في شتى المجالات، ومن بينها المجال القانوني والقضائي، لضمان سير العدالة الجنائية في نسق معتاد.

وبطبيعة الحال كان لهذا التطور الرهيب في نظم معالجة البيانات والمعلومات وتخزينها وإنتاجها، والاتساع المطرد في استخدام البريد الإلكتروني أدى بدوره إلى تطور الجرائم المرتكبة بواسطة تلك الوسائل الحديثة المتعلقة بالتحول الرقمي، لذا يجب مواجهته بتطوير المنظومة القانونية، لتواكب الثورة

التكنولوجية والتطور التقني، في مجالات المعلومات والاتصالات من جهة، وضرورة تعزيز القوانين المتعلقة بالأمن المعلوماتي من جهة أخرى وخاصة أن الابتكار الرقمي تجاوز تدابير الأمن الرقمي، من حيث الجريمة، الذي يعتبر من أبرز تحديات نظام التحول الرقمي.

أشكالية البحث:

تكمن إشكالية البحث في عدة تساؤلات نحاول من خلال هذه الدراسة الإجابة وهي كالتالي:

- ماذا نعني بالتحول الرقمي في المجتمعات؟
- كيف يمكن مواجهة الظواهر السلبية لهذا التحول من السلوك الإجرامي؟
- ما هي الجرائم المعلوماتية الناتجة عن التحول الرقمي؟
- كيف تعاملت الدول على صعيد الحماية الجنائية الموضوعية لجرائم المعلوماتية؟
- ما مدى مواكبة التشريعات الجنائية لتطور الجرائم التقنية المعلوماتية؟

منهج الدراسة:

يقوم هذا البحث في دراسته على المنهج الوصفي التحليلي.

خطة البحث:

سنحاول في هذا البحث دراسة الحماية الجنائية الموضوعية للتحول الرقمي من خلال مبحثين أساسيين:

المبحث الأول:الأحكام العامة لجرائم تقنية المعلومات في القانون الجنائي.

المطلب الأول:الجرائم المعلوماتية وخصائصها.

المطلب الثاني:التنظيم القانوني للجريمة المعلوماتية.

المبحث الثاني:الأسس التشريعية لحماية المعلومات في نظام التحول الرقمي.

المطلب الأول: التقسيم العام لجرائم المعلومات.

المطلب الثاني: تطور النصوص القانونية على الجرائم المعلوماتية.

تمهيد

مفهوم التحول الرقمي:

يستفاد من مفهوم التحول الرقمي هو كيفية استخدام التكنولوجيا داخل المؤسسات والهيئات العامة والخاصة على حد سواء، مما يساعد على رفع الكفاءة التشغيلية وتحسين جودة الخدمات التي تقدمها المؤسسات للعملاء، فهو يقوم على توظيف التقنية التكنولوجية بالشكل الإيجابي، بما يضمن توفير الجهد وحسن الخدمة[١].

إذ يرى البعض أن أحد الملامح الرئيسية للعالم اليوم هو التحول الرقمي، حيث تجاوز مستخدمو الإنترنت ما يقارب خمس مليار نسمة من سكان العالم سنة ٢٠٢٠م، وترتب عليه الانتشار الواسع لاستخدام الشبكة الدولية للإنترنت وتطبيقاتها، وقيل في بيان ماهية التحول الرقمي بأنه شكل متميز من أشكال التحول التنظيمي الذي يتم بواسطة التكنولوجيا الرقمية، وذلك بغرض توليد المعرفة التراكمية للاستفادة منها في مختلف المجالات، ويكشف التحول عن العلاقة بين التكنولوجيا والتغيير التنظيمي، واستخدام أنظمة التقنية لابتكار العمليات وتحسين الكفاءة التشغيلية للمنظومات[٢].

وللوصول إلى الكفاءة مع هذا النظام يجب صياغة استراتيجية رقمية قوية وبنية أساسية للنظام التقني للوقوف على الفجوة بين القدرات الحالية وما يجب أن يكون عليه مستقبلاً، للعمل على استخدام قنوات متطورة في تقديم الخدمة، من تطبيقات أساسية على الهواتف المحمولة مثلاً، وتوفير بعض البيانات والمعلومات الحكومية عليها، وجعلها متاحة للقطاع الخاص للاستثمار عليها، وتوفير بوابات معلوماتية بأنظمة أمن المعلومات والبيانات.

---

(١) إيهاب علي النواب، **الحكومات الإلكترونية وحتمية التحول الرقمي**، مقالات اقتصادية، شبكة النبأ للمعلومات، سنة ٢٠١٨م، ص١٢.

(٢) رزق سعد علي، **انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة**، بحث في مجلة الدراسات القانونية، كلية الحقوق، جامعة مدينة السادات، سنة ٢٠٢١م، ص١٦.

البيانات الرقمية:

تعرف البيانات ذات الطبيعة الرقمية، بكونها البيانات التي يمكن عن طريقها الاستدلال على هوية الأفراد ومؤسسات الدولة، سواء صرحت تلك القواعد الرقمية بهوية الأشخاص باسمه مثلاً، أو احتوت في مجموعها على بيانات يمكن عن طريق معالجتها تحديد الهوية، والبيانات التي تحويها المنظومات الرقمية[١].

وبهذا فإن ما يسمى بالخصوصية الرقمية هي وصف لحماية البيانات الشخصية، والتي يتم نشرها وتداولها من خلال الوسائط الرقمية وتتمثل في الحسابات البنكية الإلكترونية والبيانات الشخصية في البريد الإلكتروني، ومعلومات المؤسسات العامة والخاصة وغيرها من البيانات.

ومع هذا التنامي مع العالم الرقمي أصبحت الخصوصية مهددة وصارت البيانات مادة يتم استخدامها أو مراقبتها وتعرضها للسرقة واستغلالها في أغراض تضر بأصحابها، ولذا فإن التعامل مع التجاوزات الرقمية تحتاج إلى العديد من التوجيهات عم كيفية حمايتها، وتحديث الأطر القانونية ذات الصلة، وتوجيه السياسة الجنائية لها.

وعرّف المشرع الفرنسي البيانات الشخصية في المادة الثانية من قانون المعلوماتية والحريات الفرنسي رقم ٧٨ لسنة ١٩٧٨م المعدل بأحكام القانون الصادر في يناير ٢٠٠٢م بأنها كل المعلومات المتعلقة بشخص طبيعي محدد أو يمكن تحديده مباشرة بواسطة رقم معين أو بواسطة عنصر أو أكثر خاص به[٢].

وبناء عليه ذهبت محكمة النقض الفرنسية بأن كشف رب العمل عن موطن العامل وبياناته بدون موافقة الأخير، يعتبر اعتداء على حياته الخاصة، ويرجع أول قانون في حماية البيانات إلى مقاطعة هيسن في ألمانيا في ١٩٧٠م، والولايات المتحدة في ١٩٧٤م، وأعقب ذلك ميلاد معاهدات وقواعد إرشادية تعّد مرجعية دولية، منها المبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية والتي صدرت

(١) فرج حسن الأطرش، **نحو خلق بيئة قانونية للحكومة الإلكترونية في ليبيا**، كلية القانون، جامعة الجفرة، بحث في مجلة الجامعة، سنة ٢٠٢٠م، ص٥.

(٢) بهاء المر، **جرائم السوشيال ميديا**، دار الأهرام، القاهرة، طبعة أولى، سنة ٢٠٢٢م، ص٢٨.

عام ١٩٨٠م والمعنية بتنظيم حماية الخصوصية وتدفق البيانات عبر الحدود وكذلك اتفاقية مجلس أوروبا الصادر في عام ١٩٨١م والتي تهتم بحماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات[١].

أما التشريعات العربية كانت قاصرة في مواكبة التطور الرقمي معتمدة أساساً على القياس في بعض الجرائم المتعلقة بالمحررات الورقية، وشهدت السنوات الأخيرة صدور بعض قوانين متعلقة بالجرائم الرقمية مثل القانون المصري رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة الجرائم تقنية المعلومات، وأيضاً ما صدر عن مجلس النواب الليبي من قانون الجرائم الإلكترونية في شهر أكتوبر لسنة ٢٠٢١م الذي كان مشروع قانون سنة ٢٠١٨م ونتولى بيان ذلك من خلال هذا البحث بالشرح والتفصيل.

(١) طارق إبراهيم الدسوقي، **الأمن المعلوماتي**، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥م، ص٣٧.

المبحث الأول

الأحكام العامة لجرائم تقنية المعلومات في القانون الجنائي

تعد الجريمة الرقمية أو المعلوماتية ذات فكرة واسعة منظمة، ولها ضوابطها، وفهم العلاقة بين المعلوماتية ونظم البرمجيات، يتيح للبعض فكرة الاعتداء على تلك النظم ذات الطابع الـمُعقد، وسوف نعرض في هذا المبحث ماهية الجرائم المعلوماتية، وخصائصها في مطلب أول، والتنظيم القانوني للجريمة المعلوماتية في مطلب ثاني، وذلك علة النحو الآتي:

المطلب الأول

الجرائم الرقمية المعلوماتية وخصائصها

نقسم هذا المطلب إلى فرعين الأول متعلق بماهية الجريمة المعلوماتية، والفرع الثاني عن خصائص هذه الجريمة، وذلك على النحو التالي:

الفرع الأول: ماهية الجريمة المعلوماتية:

في مستهل الحديث عن جرائم تقنية المعلومات التي أفرزها التقدم العلمي والتكنولوجي والتقنيات عالية المستوى، من المفترض تسخيرها لخدمة المجتمعات، إلا أنها تلفقتها عقول مريضة وأنفس غير سوية، أخرجت بها من الجانب المفيد إلى الجانب المضر، وكما هو معروف أن التشريعات الجنائية لا تضع تعريفات مباشرة فهي ليست من اختصاصاتها، فهو اختصاص ففهي بحث، والجريمة المعلوماتية أو الإلكترونية هي تلك الجريمة التي ترتكب باستعمال وسائل شبكة المعلومات لتنفيذ نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أ، أي وسيلة اتصال حديثة ضد الحياة الخاصة للأفراد أو على المصالح العامة، وعرفها الفقيهان (Michel & Credo) بالتعريف الواسع بأنها باستخدام الحاسب كأداة لارتكاب الجريمة[1].

وتناول رأي من الفقه تعريفها بأنها عمل أو امتناع يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات

(١) جمال شحاتة، **قانون مكافحة جرائم تقنية المعلومات**، دار الأهرام، القاهرة، سنة ٢٠٢١م، ص٢٨.

ويفرض لها جزاء، وبالرجوع إلى مؤتمر الأمم المتحدة العاشر لمنع الجريمة المنعقد في فيينا سنة ٢٠٠٠م يتضح أنه تبنى تعريف منضبط بجريمة تقنية المعلومات بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسبي أو شبكة حاسوبية والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[١].

وذهب مكتب تقييم التقنية في الولايات المتحدة الأمريكية إلى تعريف جرائم تقنية المعلومات بأنها الجرائم التي تلعب فيها بيانات الحاسب الآلية والبرامج المعلوماتية دوراً رئيسياً.

كما عرفها خبراء منظمة التعاون الاقتصادي والتنمية (OECD) بأنها كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[٢]. ومن جانبها نرى أن تعريف الجريمة الإلكترونية هي كل سلوك إجرامي ينشأ عن الاستخدام غير المشروع لوسائل تقنية المعلومات.

الجرائم السيبرانية:

مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي وتشير المقاربة الإيثيمولوجية لكلمة (Cyber) إلى أنها لفظة يونانية الأصل مشتقة من كلمة (Kybernetes) بمعنى الشخص الذي يدير دفة السفينة حيث تستخدم مجازاً للمتحكم (Governor) وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي "Wieners" وذلك للتعبير عن التحكم الآلي في أشهر مؤلفاته، بكلمة السبرنتيقية هي التحكم والتواصل عند الإنسان والآلة، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب[٣].

الحقيقة أن هذا مصطلح هو مكمل لجرائم تقنية المعلومات إذ هو ثمرة من ثمار التقدم السريع في شتى المجالات العالمية التي يتميز بها عصرا الحالي وهي

---

(١) طارق إبراهيم الدسوقي، **الأمن المعلوماتي**، دار الجامعة الحديثة، الإسكندرية، سنة ٢٠١٥م، ص١٥٤.

(٢) عبد العزيز لطفي جاد الله، **الجريمة السيبرانية وحماية أمن المعلومات**، مؤسسة المعرفة، الإسكندرية، الطبعة الأولى، سنة ٢٠٢٢م، ص٢٢.

(٣) الطبيب مصطفى، **الفرق بين أمن المعلومات والأمن السيبراني**، مدونة العلوم السياسية، سنة ٢٠١٩م، ص٨.

ثورة في مجال الجينات والصبغات نتيجة للتقدم في فرع الهندسة الوراثية ولكن يرى جانب من الفقه أن هذا المصطلح أطلع على الجرائم الواقعة ضد الحكومات والصراع المتنامي بين الدول في سباق القطاع التقني، فالحق المعتدي عليه يمثل الدولة باعتبارها، الشخص القانونية التي يمثل المجتمع في حقوقه ومصالحه كافة[١].

ويرى البعض أن هذه الجريمة هي مجموعة رموز يستخلص منها معنى معين في مجال محدد وتتمتع بالتحديد والابتكار والسرية الاستئثار، وتتميز أيضاً بأنها عابرة للحدود وقد تكون منظمة في هيئة شركات متخصصة تدير هذا النوع من الجرائم، وهذا النوع يتطلب المهارة والتنظيم والوسيلة المكلفة والسلطة والمعرفة، وأيضاً البنية الأساسية وهي جميع ما يستعمل أو يكون معداً للاستعمال في الاتصالات والنظم والبرامج[٢].

وفي التقرير الصادر عن الاتحاد الدول للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام ٢٠١١م عُرف الأمن السيبراني بأنه: مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[٣].

الفرع الثاني: خصائص جرائم المعلوماتية:

تتشابه الجريمة المعلوماتية مع الجريمة العادية في أن لكل منهما أركان وفق القواعد العامة متمثلة في الركن المادي، وعدم المشروعية، والركن المعنوي الإرادة الأثمة، ويمكن الاختلاف بينهما في أداة ارتكاب الجريمة، إذ أن الفضاء المعلوماتي هو مكان الجريمة الإلكترونية، الذي لا يتطلب انتقال المجرم إليها، وإنما يرتكبها من خلال الضغط على أزرار جهازه، الذي يتصل بشبكات الإنترنت، ولهذا تكمن

(١) عمر محمود الحوثي، **الموجز في الحماية الجنائية في جرائم تقنية المعلومات**، دار النهضة العربية، القاهرة، سنة ٢٠٢١م، ص٢٣.

(٢) عبد العزيز لطفي جاد الله، المرجع السابق، ص٣٤-٣٥.

(٣) الطبيب مصطفى، مرجع سابق، ص١٢.

خطورتها.

ومن هنا يمكن إجمال خصائص هذا النوع من الجرائم في النقاط التالية:

١. أن لكل مرحلة من مراحل المعالجة الآلية للبيانات (الإدخال والمعالجة، والإخراج) نوعية خاصة من الجرائم، لا يمكن بالنظر لطبيعتها ارتكابها إلا مع وقت محدد، وهذه خاصية من حيث موضوع الجريمة.

٢. إن هذا النوع من الجرائم يضفي أبعاداً غير مسبوقة في الضرر، ويلحق خسائر عالية وفق تقديرات المركز الوطني لجرائم الحاسب الآلي في الولايات المتحدة الأمريكية[١].

٣. تمتاز هذه الجرائم بصعوبة الاكتشاف، إذ هي مجرد أرقام وببيانات تتغير أو تمحى من السجلات المخزنة في المنظومات التقنية، فلا تترك أثر خارجياً مرئياً.

٤. أن هذا النوع من الجرائم تميز أيضاً بتخطيها للحدود الجغرافية، ومن ثم اكتسابها الصبغة الدولية.

٥. تتميز الجريمة المعلوماتية عادة، أنها تتحقق بتعاون أكثر من شخص على ارتكابها، وغالباً ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في هذه التقنية، والجانب الفني من المشروع الإجرامي[٢].

٦. سهولة إخفاء معالم الجريمة وصعوبة تتبع مرتكبيها، نظراً لكون مسرح الجريمة داخل عالم من الأنظمة الرقمية وليس بالمسرح التقليدي، وكذلك إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة وجيزة[٣].

---

(١) طارق الدسوقي، **الأمن المعلوماتي**، مرجع سابق، ص١٦٤.

(٢) عمر محمود الحوثي، **الوجيز في الحماية الجنائية في جرائم تقنية المعلومات**، مرجع سابق، ص٢٧.

(٣) عبد العزيز لطفي جاد الله، **الجريمة السيبرانية**، مرجع سابق، ص٣٢.

المطلب الثاني

التنظيم القانوني للجريمة المعلوماتية

لبسط الحماية الجنائية المعلوماتية وتحقق أهدافها على الجانب الموضوعي، فإن الحماية الجنائية تنطوي على تأمين استثمارات تكنولوجيا المعلومات في جوانبها المتعددة سواء المادية أو البشرية، مما يشجع على فكر الابتكار، ويدفع بالتقدم العلمي في ظل نظام التحول الرقمي للدول.

وقد كانت جل التشريعات تنظم الجوانب القانونية لمواجهة الإجرام المعلوماتي بمجموعة القواعد العامة المطبقة على الجرائم التقليدية، إلى إن أصدرت بعض الدول قوانين خاصة تنظم هذه الجرائم.

وسوف نتناول موضوع التنظيم القانوني للجريمة المعلوماتية من خلال فرعين الأول متعلق بالطبيعة القانونية، والفرع الثاني في كون المعلومة مالاً يستحق الحماية.

الفرع الأول: الطبيعة القانونية للمعلوماتية في نظام التحول الرقمي:

يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج المعلوماتية، وهل لها قيمة من ذاتها، أم أن قيمتها تتمثل في أنها مجموعة مستحدثة من القيم القابلة للاستثناء يمكن الاعتداء عليها؟

ووفقاً للقواعد العامة، فالأشياء المادية وحدها التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون كيان مادي ملموس حتى يمكن انتقاله وحيازتها عن طريق الاختلاس المكون للركن المادي لجريمة السرقة، ولما كانت المعلومة ذات طبيعة معنوية لا يمكن اعتبارها إلا من قبيل حقوق الملكية الفكرية، وتثور المشكلة عندما نكون أمام سرقة مال معلوماتي غير مادي، أي لم تكن مسجلة على أسطوانة أو مدونة.

وتعتمد تقنية المعلومات في انتشارها على أنظمة الاتصالات، فكلما تقدمت هذه الأنظمة وارتقت كلما أتيح للمجتمع أن ينمو ويتطور، ولذا أصبحت قيمة غير تقليدية جديرة برفعها إلى مصاف القيمة المادية، فيتحدد سعرها بوصفها سلعة قابلة

للتداول، خاضعة لظروف العرض والطلب تباع وتشترى، في سوق يدور فيه الصراع حول هذا المنتج بمبالغ هائلة، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم عرفت بالجرائم المعلوماتية.

الملكية في فضاء المعلومات:

نظراً لغياب الطبيعة المادية للمعلومات، أصبح الفقه الجنائي يواجه تحدياً كبيراً في الملكية المعلوماتية، وبالتالي إمكانية خضوعها للحماية الجنائية[١].

فذهب رأي إلى أن مستحدثات العصر والتقنيات الحديثة أظهرت ما عرف بالمال الإلكتروني وهذا المال يمكن تملكه، ولو كان هناك خلاف حول طبيعة هذا المال هل هو مادي أم معنوي، ولكن الثابت أن هذه الأموال معرضة للاعتداء عليها، ولذا يجب أن تتعامل بوصفها قيمة وتصبح محلاً للحق[٢].

فالمعلومة عندما يتم استخدامها فإنها تخص مالكها، ولا يجوز الاعتداء عليها.

بينما يذهب رأي آخر ينفي الحق في الملكية على المعلومة، مؤسساً ذلك على ما أسماه بنظام السماء المفتوحة، متمسكاً بمذهب الحرية في الاقتصاد الإلكتروني فالمعلومة لا تقبل التملك والاستثمار، فالانتفاع بها حق للكافة، والمعلومات لا يمكن احتكارها، وبالتالي لا يمكن تملكها، فالأفكار تسير كما تشاء[٣]، لكن هذا الرأي تعرض لانتقادات جمة، لأن جل التشريعات تعترف بالحقوق الفكرية.

الفرع الثاني: تقنية المعلومات مالاً يستحق الحماية الجنائية:

ظهرت فكرة الأموال القانونية على يد الفقيه الألماني (فون ليست)، الذي قال أن قانون العقوبات يستهدف حماية أموال معينة، يرى المشرع جدارتها بالحماية الجنائية، وتناولها الفقيه الإيطالي (روكو) وعرفها بأنها كل ما من شأنه إشباع

(١) حساب عامل الأهواني، **الحماية القانونية في مواجهة الحاسب الآلي**، بحث مقدم في مؤتمر الكويت الأول، سنة ٢٠٠٠م، ص١٦.
(٢) طارق الدسوقي، مرجع سابق، ص٢٤١.
(٣) المرجع نفسه، ص٢٤٢.

حاجة معينة[١].

والمال في القانون المدني هو كل شيء يصلح في ذاته لأن يكون محلاً لحق مالي، يدخل في تقدير ذمة شخص طبيعي أو اعتباري، بمعنى أنه كل شيء قابل للتقويم، ويكون الشيء كذلك إذا صلح محلاً لحق من الحقوق المالية.

ويشترط أن يكون المال غير خارج عن دائرة التعامل بطبيعته أو بحكم القانون، وهذا الشرط غير موجود في القانون الجنائي، إذ لا يشترط فيه أيضاً أن يكون ذا قيمة يمكن التعبير عنها بالنقود، فالمال في القانون الجنائي ينظر إليه من نطاق القيمة التي يمثلها المال[٢].

اختلف الفقه في مسألة اعتبار المعلومات أموالاً تستحق الحماية أم لا، وذهب الرأي الأول إلى أن المعلومات لا تعتبر مالاً وليس لها طبيعة مادية، فالأشياء المحسوسة هي التي تعتبر من قبيل الأشياء المادية، فعدم مادية المعلومة هو الذي أدى بهذا الرأي إلى استبعادها من طائفة الأموال.

فبرامج المعلومات أمر ذهني، وهي تدخل ضمن الأحكام الخاصة بحماية الملكية الفكرية، والمعلومة بعيداً عن دعائمها لا تقبل التملك والانتشار فالانتفاع مباع للكافة[٣].

إلا أن استبعاد المعلومات عن نطاق القيم المادية لم يمنع الفقه والفضاء الفرنسي من محاولة إيجاد حماية قانونية لها في حالة الاستيلاء غير المشروع عليها، واتخذت فيما قبل أشكال مختلفة مثل الاستعانة بدعوى المنافسة غير المشروعة، وتأسيس الخطأ على نظرية الإثراء بلا سبب، أو المسئولية التقصيرية.

الرأي الثاني اعتبر المعلومة مالاً مادياً في حد ذاتها، وسنده في ذلك أنه لا يجوز الخلط بين طبيعة حق صاحب الشيء وطبيعة الشيء ذاته، فليس بالضرورة إذا كانت طبيعة حق الشيء معنوية أن تكون طبيعة هذا الشيء ذاته معنوية، ويفصل

(١) إبراهيم عبد الخالق، **جرائم الأموال - الجزء الثاني**، المكتب الفني للإصدارات القانونية، القاهرة، الطبعة الثالثة، سنة ٢٠٢٠م، ص١٦.

(٢) المرجع نفسه.

(٣) إبراهيم الدسوقي، مرجع سابق، ص٢٥١.

في ذلك هو تحديد كلمة المادة في العلوم الطبيعية، إذ هي كل شيء يشغل حيزاً مادياً في فراغ معين، يمكن قياسه أو التحكم فيه، وبالتالي فالبيانات الإلكترونية تشغل حيزاً يمكن قياسه بوحداته الخاصة، فهي كالتيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من الأشياء المادية[١].

فالمعلومة طائفة جديدة من الأموال مما يمكن أن ترد عليها الحقوق المالية، واعتبارها جزء من الذمة المالية للشخص، فلا تميز بين الاعتداء على الذمة المالية، وبين الاعتداء الذي يقع على المعلومات أو البيانات، التي أصبحت ذا قيمة مالية تكون محلاً لعقد البيع[٢].

إن التحليل المنطقي يفرض الاعتداد بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي للبرامج، وأنها لا يمكن أن تكون شيئاً ملموساً، ولكن لهما كيان مادي قابل للانتقال والاستحواذ عليه، بتشغيل جهاز ورؤية المعلومات على الشاشة، مترجماً إلى أفكار تنتقل من الجهاز إلى ذهن المتلقي، وهذه المعلومات يتم نقلها بواسطة رموز وشفرات يمكن حلها إلى بيانات معينة لها أصل صادرة عنه يمكن سرقته وبالتالي لها كيان مادي يمكن الاستحواذ عليه.

(١) طارق إبراهيم، مرجع سابق، ص٤٠.

(٢) جميل عبد الباقي الصغير، **القانون الجنائي والتكنولوجيا الحديثة**، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة ١٩٩٢م، ص٥٧.

المبحث الثاني

الأسس التشريعية لحماية المعلومات في نظام التحول الرقمي

يتطلب التحول الرقمي إلى تغييرات شاملة في أطر مختلفة، ومنها الإطار التشريعي القانوني، والنظام القضائي للدول، وإذا كان انخراط المجتمعات وجل مؤسساتها وأفرادها في التحول المعلوماتي الحديث، أمراً محموداً، إلا أن هناك أنماطاً من السلوك الإجرامي تظهر على هذا التغيير، حيث تساعد تلك الوسائل الحديثة على توسيع عمليات انتهاك الخصوصية العامة والخاصة، معتمدة على معطيات البيئة الرقمية، وترتب على ذلك الرغبة الملحة في تطوير البنية التشريعية ذات الصلة بالجرائم الرقمية[١].

وسنتناول الحديث عن هذه البنية التشريعية في هذا المبحث من خلال مطلبين الأول نخصصه لتقسيم جرائم المعلومات والثاني عن تطور الدول في مجال النصوص القانونية والقوانين الخاصة لجرائم المعلومات في القانون الفرنسي والتشريع المصري والليبي وذلك على النحو التالي:

(١) رزق سعد علي، **انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة**، بحث في كلية الدراسات القانونية، كلية الحقوق، جامعة مدينة السادات، سنة ٢٠٢١م، ص٥٠.

المطلب الأول

التقسيم العام لجرائم المعلومات

يقصد بتقسيم جرائم المعلومات هو بيان الموضوعات والأنشطة الإجرامية التي تدخل ضمن إطارها، وذلك لتحديد مدى الأضرار الناجمة عنها، ودرجة الجسامة، بحيث يتم توجيه السياسة الجنائية في مكافحتها ووضع آلية الجزاء المناسب لها، وسنحاول بيان هذا التقسيم من خلال الفرعين التاليين:

الفرع الأول: التقسيم الفقهي لجرائم المعلوماتية:

ذهب جانب من الفقه إلى تقسيم جرائم المعلومات إلى ثلاثة أقسام:

جرائم الحاسب الآلي الاقتصادية:

تعتمد هذه النوعية من الجرائم القسم الأساسي لجرائم المعلومة وتندرج تحتها:

- الاحتيال المعلوماتي وهو التلاعب في المعلومات للحصول بغير حق على منفعة.
- التجسس المعلوماتي وهو اختراق البيانات من أجل الوصول إلى معلومات مخفية.
- إتلاف المعلومات سواء بالمكونات المادية المتصلة بتقنية المعلومات أو غير مادية متعلقة بإتلاف البيانات المدخلة على الأنظمة الإلكترونية.
- سرقة الخدمات والاستفادة والاستيلاء على الخدمة إلكترونياً.
- جريمة الانتفاع بدون وجه حق بخدمات التقنية والاتصالات[1].

الجرائم المتعلقة بانتهاك الحياة الخاصة:

بدء ظهور الاهتمام بحماية الحياة الخاصة من الاعتداءات المعلوماتية بعد انتشار أنواع مختلفة من الجرائم الماسة بالحياة الخاصة، وتناول الفقه أربعة أقسام

(١) عمر محمود الحوثي، **الوجيز في الحماية الجنائية من جرائم تقنية المعلومات**، مرجع سابق، ص٦٩.

من تهديد الحياة الخاصة نمثله في:

- استخدام بيانات شخصية غير صحيحة.
- الإفشاء غير المشروع للبيانات الشخصية.
- جمع وتخزين البيانات الصحيحة بشكل غير مشروع.
- مخالفة القواعد والإجراءات الشكلية للخصوصية[١].

الجرائم التي تهدد المصالح القومية:

وهي جرائم متعلقة بالأمن القومي للدول تشمل الاعتداء على أنظمة الدفاع في الدولة، وأنظمة القوات المسلحة والجيوش، وأنظمة الطيران.

الفرع الثاني: التقسيم الدولي للجريمة المعلوماتية:

المجلس الأوروبي والجريمة الإلكترونية:

في هذا الصدد استهل المجلس الأوروبي دراسته بخصوص الجرائم الإلكترونية المرتبطة بالحاسب الآلي برؤيته لتطوير سبل مكافحة هذا النوع من الجرائم، ولمساعدة سلطات التشريع في الدول الأعضاء بشأن تحديد طبيعة الجريمة المعلوماتية، والتي ينبغي تجريمها قانوناً وسن عقوبات رادعة لها.

وقد تبنى المجلس الأوروبي عدة توصيات في أولى اجتماعاته سنة ١٩٨٩م، حيث تم إدراج طائفتين من التجريم الأولى تضم القائمة الأساسية لإلزامية، وتشمل الاحتيال المعلوماتي، والتزوير، والإتلاف، والاعتراض غير المصرح به لنظام الحاسب، وإعاقة النظم عن الوظيفة، والدخول غير المشروع للنظام المعلوماتي والنسخ غير المشروع للبرامج.

أما الطائفة الثانية تضم مجموعة الأفعال الاختيارية، وهي متعلقة بالتعديل في البيانات المخزنة بالحاسب، وذلك في الحالة التي لا يؤدي فيها هذا التعديل إلى الإتلاف، والتجسس المعلوماتي، والاستعمال غير المصرح به لنظام الحاسب الآلي[٢].

---

(١) عمر محمود الحوثي، **الوجيز في الحماية الجنائية من جرائم تقنية المعلومات**، مرجع سابق، ص٦٩.

(٢) طارق الدسوقي، مرجع سابق، ص٢١٥.

وحيث عقد المجلس الأوروبي سنة ١٩٩٥م مؤتمراً وأصدر توصية بأن التطور في نظم المعلومات الإلكترونية، سوف يعجل بتحول المجتمع التقليدي إلى مجتمع معلوماتي (وهو التحول الرقمي اليوم) من خلال إيجاد فضاء جديد لكل أنواع الاتصالات، والعلاقات بين الأفراد والمؤسسات العامة والخاصة[١].

اتفاقية بودابست ٢٠٠١م:

تصدت هذه الاتفاقية للاستخدام غير المشروع للحاسبات وشبكات المعلومات ونصت في الباب الثاني من الاتفاقية، على تحسبن وإصلاح وسائل منع وقمع الإجرام المعلوماتي، وذلك من خلال تحديد معيار بالحد الأدنى الذي يسمح باعتبار بعض التصرفات من قبيل الجرائم الجنائية، وتسهيل مكافحة هذا النوع من الجرائم. وتشير المذكرة التفسيرية للاتفاقية إلى أن قائمة الجرائم مدرجة في هذا الباب القسم يمثل الحد الأدنى للتوافق الذي لا يستبعد أن يتم استكمال هذه القائمة في القانون الداخلي، وأن هذه القائمة تستند إلى المبادئ المنصوص عليها من المجلس الأوروبي بخصوص الجرائم المتعلق بالحاسب الآلي المشار إليها أنفاً[٢].

اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية فيينا ٢٠١٥م:

قرر مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية، أن تنشئ فريق عمل مفتوح العضوية، ووضع هذا الفريق عدة توصيات منها:

١. تبادل الأدلة الإثباتية الإلكترونية للمساعدة في الأنشطة التقنية.

٢. إدراج المعلومات والمواد ذات الصلة في بوابة إدارة المعارف، المعروفة بوابة الموارد الإلكترونية والقوانين المتعلقة بالجريمة.

٣. تعميم القوانين الوطنية والإرشادات والمبادئ التوجيهية ذات الصلة.

٤. التعاون في المسائل الجنائية بما فيها وضع الصيغ النهائية لطلبات المساعدة

---

(١) المرجع نفسه، ص٢١٧.

(٢) مجلس أوروبا، **الاتفاقية المتعلقة بالجريمة الإلكترونية**، بودابست، سنة ٢٠٠١م، شبكة المعلومات الإنترنت.

القانونية المتبادلة المنقحة[١].

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ٢٠١٠م:

تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدون العربية وكانت في سنة ٢٠١٠م بالقاهرة وذلك في مجال مكافحة جرائم المعلومات، لدرء مخاطرها بين الدون العربية وسلامة الدول مجتمعاتها.

وتضمنت هذه الاتفاقية بنود عدة في مجال التحقيق الجنائي، وملاحقة مرتكبي الجرائم مثل الاعتداء على سلامة البيانات، وجرائم إساءة استعمال وسائل تقنية المعلومات، والتزوير، والاحتيال، والجرائم المتعلقة بالحياة الخاصة، ومكافحة الإرهاب، وتمويله، والدعوة لأفكاره، وكذلك جرائم غسيل الأموال والإتجار بالبشر والأسلحة.

(١) **مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة**، سنة ٢٠١٥م، فيينا، موقع الأمم المتحدة عبر شبكة المعلومات، ص٢-٣.

المطلب الثاني

تطور النصوص القانونية على الجرائم المعلوماتية

بعد هذا التطور الهائل في السبل المعلوماتية، بحيث أصبحت أساساً في وسائل ارتكاب الجرائم ضد الأشخاص والأموال، وأن السلطات العامة في الدولة ذاتها من الممكن أن تستخدم هذا الفضاء في الإفتات على حريات وحقوق الأفراد، أصبح لزاماً التخلي عن أسلوب القياس بالجرائم التقليدية مع القواعد العامة في قانون العقوبات، والبحث عن أسلوب تشريعي لحماية المصالح الخاصة والعامة، وذلك بسن قوانين عقابية يقرها المشرع.

وظهرت في فرنسا أولى مراحل هذا القانون في يناير ١٩٧٨م بصدور قانون متعلق بالمعلوماتية والحريات، واقتصر على حماية الحياة الخاصة الشخصية وجاء تعديل آخر في يناير ١٩٨٨م تحت عنوان بعض الجرائم في مواد المعلومات، كان الهدف منه هو ردع الدخول غير المشروع على برامج المعلوماتية، بمعنى حماية النظام المعلوماتي ذاته ضد أي اعتداء خارجي، ومع تزايد الاهتمام من المشرع الفرنسي فقد تم تعديل في قانون العقوبات وتضمينه أحكام جديدة في عام ١٩٩٤م في الفصل الثالث، تحت عنوان الاعتداءات على نظم المعالجة الآلية للمعلومات[١].

ولم يقف المشرع الفرنسي عند هذا الحد أمام التحول الرقمي المأهول داخل المجتمع وتعدد مظاهره، فقد جاء بتعديل لبعض النصوص المتعلقة بالجرائم الرقمية في عام ٢٠٠٤م، فشدد العقوبات على الدخول غير المشروع في النظام التقنين وخاصة إذا ترتب على الدخول غير المشروع تعديل أو محو المعلومات المخزنة، وكذلك بعض صور الحماية الجنائية الخاصة، فنص على اعتبار الخصاص الوراثية من البيانات الشخصية، والحق في الصوت والصورة، كأحد المفردات الشخصية، وأيضاً حماية الرقم القومي، وأرقام بطاقات الائتمان، وأيضاً نص القانون رقم ٤٩٣ لسنة ٢٠١٨م الصادر في يونيو ٢٠١٨م على اعتبار المعلومات المتعلقة بالحالة الصحيحة للإنسان من البيانات الشخصية، التي تدخل ضمن نطاق الحماية

(١) طارق إبراهيم الدسوقي، مرجع سابق، ص٢٥٧-٢٥٨.

القانونية[١].

هكذا حاول جاهداً المشرع الفرنسي إحاطة صور الاعتداء الحديث على البيانات والمعلومات التقنية، ليكفل توفير بيئة مناسبة للعمل في المجال الرقمي محاطة بحماية جنائية تجرم وسائل الاعتداء غير المشروع.

الفرع الأول: التشريع المصري وجرائم المعلومات:

كان المشرع المصري إلى جانب التشريعات الأخرى لا يوجد به نظام قانوني خاص بجرائم المعلومات، وظلت هذه الجرائم رغم تزايد الشعور بأهمية تجريمها متروكة لاجتهاد الفقه والقضاء، حيث حاول كل منها عن طريق القياس تبرير تطبيق القواعد الموضوعية والإجرائية المتعلقة بالجرائم العادية على الجرائم المعلوماتية، وواقع الأمر أن القواعد القانونية التي يحاول الفقه والقضاء ثني رقبتها لكي تنطبق على جرائم المعلومات تشمل طائفتين:

الأولى: تشمل القواعد الموجودة خارج إطار قانون العقوبات ولكنها تفرض نوع من الحماية الجنائية ضد فعال شبيهة بالجريمة المعلوماتية، مثل القواعد الخاصة بالحماية الجنائية لحقوق المؤلف، وقانون التوقيع الإلكتروني سنة ٢٠٠٤م، وبشأن هذه الحقوق الدينة تنص المادة ٨٦ من القانون المدني المصري: على أن الحقوق التي ترد على شيء غير مادي تنظمها قوانين خاصة.

الثانية: تشمل القواعد التي يحتويها قانون العقوبات من الجرائم الخاصة بالسرقة والتزوير وخيانة الأمانة وغير ذلك من الأفعال المجرمة للقياس عليها في جرائم المعلومات[٢].

وسار المشرع المصري طيلة الحقبة الزمنية الماضية في تسلسل تشريعي يقترب شيئاً فشيئاً حول وجود إطار قانوني ينظم كل ما له علاقة بالطور التقني، وذلك بقوانين خاصة جاءت على فترات زمنية على النحو التالي:

(١) رزق سعد علي، مرجع سابق، ص٢٨.

(٢) طارق الدسوقي، مرجع سابق، ص٢٦٣-٢٦٤.

١. القانون رقم ١٣٢ لسنة ١٩٤٩م بشأن براءات الاختراع والرسوم والنماذج الصناعية:

حيث ذهب جانب من الفقه المصري إلى أن نصوص هذا القانون تنطبق على الجانب المادي من نظام المعالجة الآلية للمعلومات، ولكن ألغي هذا القانون بصدور قانون جديد ينظم حماية الحقوق الفكرية، وألغي أيضاً قانون رقم ٣٥٤ لسنة ١٩٥٤م بشأن حماية حق المؤلف.

٢. قانون رقم ٨٢ لسنة ٢٠٠٢م بإصدار قانون حماية حقوق الملكية الفكرية:

تضمن هذا القانون براءات الاختراع ونماذج المنفعة، وكيفية استغلالاها وحصول تراخيص لها، وكذلك حقوق النشر والرسم والمخطوطات، وأيضاً نشر وصف أو تسجيل صوتي أو برنامج إذاعي عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكة المعلومات أو غيرها من الوسائل بدون أذن كتابي مسبق من المؤلف.

٣. القانون رقم ١٥ لسنة ٢٠٠٤م بشأن تنظيم التوقيع الإلكتروني:

ضم هذا القانون ٣٠ مادة معنية بالمعاملات الإلكترونية وتكنولوجيا المعلومات، وبتنظيم التوقيع الإلكتروني، وإنشاء هيئة تنمية صناعة التقنية والمعلومات، وكان لهذا القانون صدى واسع في حسم العديد من الإشكاليات القانونية المتعلقة بالمعاملات الإلكترونية، التي كانت تدور في فكر اجتهاد الفقه والقضاء.

٤. القانون رقم ١٧٥ لسنة ٢٠١٨م قانون مكافحة جرائم تقنية المعلومات:

صدر هذا القانون بعد تزايد الاعتداءات المختلفة على الصعيدين العام والخاص، وبعد مخاض عسير أحسن المشرع المصري بإصدار هذا القانون، لمعالجة النقص التشريعي في بعض الوقائع المستحدثة، وأعطي هذا القانون دور وقائي للأجهزة المختصة من خلال الرصد والمتابعة لمواقع التصفح العامة المحرضة على الأفعال غير المشروعة.

يحقق هذا القانون التوزان بين مكافحة الاستخدام غير المشروع للحاسبات

وشبكات المعلومات وحماية البيانات والمعلومات الحكومية الخاصة بالدولة، وحماية حرمة الحياة الخاصة، وقد ضم هذا القانون عدد ٤٥ مادة، حيث نسرد أهم ما جاء فيه:

- التزامات مقدم الخدمة.
- التعاون الدولي في مكافحة جرائم تقنية المعلومات.
- جرائم الاعتداء على سلامة شبكات وأنظمة المعلومات.
- الدخول غير المشروع والانتفاع بدون حق.
- الاعتداء على سلامة البيانات والبريد الإلكتروني والمواقع الخاصة.
- الاعتداء على أنظمة معلومات الدولة.
- جرائم الاحتيال والاعتداء على البنوك.
- جرائم الاعتداء على حرمة الحياة الخاصة.

٥. قانون حماية البيانات الشخصية رقم ١٨١ لسنة ٢٠٢٠م:

والذي يعتبر من القوانين المتخصصة في حماية المعلومات الشخصية، داخل النظام التقني، ولزيادة الخطورة وتعدد ظواهر السلوك الإجرامي، بدء المشرع في إجراء بعض التعديلات على قانون العقوبات، والذي نص على إضافة مادة رقم ١٨٦ مكرر لقانون العقوبات، تجرم التصوير في المحاكمات الجنائية ونشرها على وسائل التواصل الاجتماعي.

والقانون رقم ١٤١ لسنة ٢٠٢١م والخاص بتعديل بعض نصوص قانون العقوبات المتعلق بالتحرش، والذي أدرج ضمنه التحرش الجنسي بوسائل إلكترونية، كصورة من صور التحرش.

وبذلك يكون المشرع المصري يحاول مواكبة تطور الجرائم الإلكترونية بأن لا يكون هناك فراغ تشريعي لمثل هذه الوقائع.

الفرع الثاني: التشريع الليبي وجرائم المعلوماتية:

لم يواكب التشريع الليبي متطلبات التطور الرقمي، وظهر إلى وقت قريب يعتمد على القياس في الجرائم الإلكترونية معتمدًا على اجتهاد الفقه والقضاء، كما كان في جل التشريعات، رغم صدور عدة قوانين خاصة، وبالبحث في التشريعات

العامة بالجريدة الرسمية الليبية، منذ أن صدرت في بداية خمسينيات القرن الماضي وهي تمثل الفكر القانوني السائد من قانون العقوبات والإجراءات الجنائية والقانون المدني وقانوني المرافعات لا تجَّد ما يشير إلى هذا النوع من الجرائم المتعلقة بالتقنية المعلوماتية، إلا من خلال نصوص يتم القياس عليها متعلقة بالوثائق الورقية، وهذا أسلوب منتقد في القانون الجنائي، مثل التزوير وجريمة التشهير إذا حصل عن طريق الصحف أو غيرها من الطرق العلانية، فإن العلانية يمكن أن تتصرف إلى جريمة الشبكات إذا اشتغلها الفاعل بالتشهير، كما يحصل في صفحات التواصل الاجتماعي.

أما فيما يتعلق بالتشريعات الخاصة وهي التي تتعلق بجرائم معينة، وتصع لها قواعد خاصة، ولا يرجع للتشريعات العامة إلا عند عدم وجود النص الخاص بها، نستعرض لها حسب تسلسلها التاريخي.

١. قانون حماية حق المؤلف رقم ٩ لسنة ١٩٦٨م.

حيث نص هذا القانون على حماية مؤلفي المصنعات المكتوبة، والرسم والتصوير والنحت، والمصنعات التي تلتقي شفوياً بالمحاضرات والخطب والمسرحيات[١].

٢. القانون رقم ٧٦ لسنة ١٩٧٢م بشأن المطبوعات.

شمل هذا القانون المطبوعات وهي جميع الكتابات والرسوم والصور المطبوعة سواء دورية أم شبه دورية، يتم تداولها كالصحف والجرائد وغيرها[٢].

في هذا الإطار أثار البعض مسألة اعتبار المكونات الإلكترونية مدونات مطبوعة أم لا، والمدونة حقيقة هي صحيفة ينشئها صاحبها بقصد التداول، ونشر الأفكار التي تتضمنها على نطاق واسع، وكذلك الأمر بالنشر في شبكات التواصل والمنتديات الإلكترونية التي أصبحت أكثر انتشاراًن إلا أن العائق في هذا القانون هو المادة العاشرة التي تشترط الترخيص، ومن حق إدارة المطبوعات رفض

(١) **منظومة التشريعات الليبية**، ص٨٨.

(٢) المرجع نفسه، ص٩٩.

الترخيص وهذا يدل على أن القانون صيغ على ما هو مطبوع ورقياً بعيداً عن التواصل المعلوماتي الحديث.

٣. القانون رقم ٢٧ لسنة ١٩٨٥ بشأن إنشاء المركز الوطني للمعلومات والتوثيق.

أوكلت لها المركز عدة اختصاصات مهمة في عالم التقني في جمع المعلومات وحفظها، وفقاً للأسس والوسائل التقنية الحديثة وجعلها في متناول الجهات العامة، والمساهمة في كل ما من شأنه تنمية حركة المعلومات والتوثيق.

- إقامة قواعد ومصادر معلومات وطنية في مجالات الطاقة والعلوم التقنية.
- الإشراف على استخدام الحاسبات الآلية وتوجيهها[١].

٤. القانون رقم ٤ لسنة ١٩٩٠م بشأن النظام الوطني للمعلومات والتوثيق.

حيث نص هذا القانون في مادته الثالثة على أن يشمل النظام الوطني للمعلومات والتوثيق عدة بيانات نذكر بعض منها:

- الإحصائيات والبيانات والمعلومات بكافة الأنشطة في مؤسسات الدولة.
- التقارير والدراسات والبحوث متعلقة بمختلف المجالات.
- الخرائط والرسومات والمواصفات الفنية للعقود المبرمة لتنفيذ المشروعات.
- كافة القوانين والقرارات واللوائح الرسمية.
- الأحكام القضائية النهائية الصادرة من المحاكم في الأحوال الشخصية والمسائل الجنائية[٢].

يلاحظ على القوانين المذكورين أنفًا، كانا في بداية عهد انبلاج ثورة المعلومات، حيث كان يمكن أن تكون بداية جيدة في وقت مبكر لزمن تقنية المعلومات، بإنشاء هذا المركز، إلا أنه من خلال البحث والتقصي في الواقع العملي لهذا المركز، بأنه لم يؤدي عمله أساسًا، وفق تلك القوانين، فلم يتحصل على الدعم الكافي، ووقع في دائرة البيروقراطية السائدة في مجتمعاتنا فكانت هذه القوانين مجرد حبر على ورق لم ترى النور أساساً، ولو أدى هذا المركز اختصاصاته على

(١) **منظومة التشريعات الليبية**، مرجع سابق.

(٢) المرجع نفسه.

النحو الوارد في قانونه لكان بداية مثالية لعصر المعلومات وتجربة يشاد لها بلبنان، ونقلت المجتمع بالشكل المطلوب للتطور التقني للعالم.

٥. القانون رقم ١ لسنة ٢٠٠٥م بشأن المصارف.

أهم ما أشار إليه هذا القانون في مجال التوقيع الإلكتروني على النحو التالي:

- يعتمد بالمستندات والتوقيعات الإلكترونية التي تتم في إطار المعاملات المصرفية وتكون لها الحجية في إثبات ما تتضمنه من بيانات.
- تعتبر مخرجات الحاسوب المتعلقة بالمعاملات المصرفية بمثابة دفاتر قانونية[١].

ويعتبر في هذا القانون قفزة كبيرة ومتقدمة في الأخذ بتقنية العصر الحديث، حيث أعتد بالمستندات الإلكترونية وتوقيعاتها، وأعطتها الحجية الكافية في الإثبات.

إلا أنه يعيب هذا القانون اقتصاره على المعاملات المصرفية فقط.

٦. القانون رقم ٢٢ لسنة ٢٠١٠م بشأن الاتصالات.

وهو قانون ينظم قطاع الاتصالات، حيث أنه أشار إلى بعض العقوبات الجنائية على سبيل الاحتياط، وقد حددت المادة ٣٥ من هذا القانون عقوبة إساءة استخدام شبكة المعلومات الدولية، إذ يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن ثلاثة آلاف ولا تزيد عن خمسة آلاف، وسحب التراخيص ومصادرة الآلات كل من أساء استخدام شبكة المعلومات الدولية في نشر المعلومات أو بيانات تمس الأمن السياسي أو الاقتصادي أو الاجتماعي للمجتمع العربي الليبي أو استخدام الفيروسات لإيذاء الغير[٢].

ربما يعتبر هذا النص الخاص بداية إحساس المشرع بخطورة التقنية المعلوماتية إلا أن هذا النص لا يغطي كافة أنواع السلوك الإجرامي المتعلق

---

(١) **منظومة التشريعات الليبية.**

(٢) المرجع نفسه.

بالمعلوماتية.

٧. قوانين أخرى تعلقت بحجية التوقيع الإلكتروني والمستندات التجارية الإلكترونية.

وهي قانون النشاط التجارية رقم ٢٣ لسنة ٢٠١٠م في مادته ٤٦٣ المتعلقة بالمستندات المحاسبية الإلكترونية، وأيضاً القانون رقم ١٧ لسنة ٢٠١٠ بشأن التسجيل العقاري في مادته ٧٠، ٧١ بشأن التوقيع الإلكتروني والكتابة الإلكترونية، وتمتعها بنفس قوة الكتابة العادية وكذلك القانون رقم ١١ لسنة ٢٠١٠م بشأن سوق المال المادة رقم ٩٥ بشأن التوقيع الإلكتروني.

يلاحظ أن سنة ٢٠١٠م كانت بداية التحول الأساسي للمشرع نحو الاعتراف بالمعاملات الإلكترونية وذلك بسن عدة قوانين تعّير في طياتها، ولو بشكل ضئيل إلى التحول الرقمي داخل مؤسسات الدولة.

وبعد ما شهدت ليبيا من أحداث عقب الثورة، وعدم استقرار الدولة على مستوى السلطات الثلاثة التشريعية التنفيذية القضائية، ظل مشروع قانون الجرائم الإلكترونية مجرد مسودة إلى أن تم اعتماده مؤخراً من قبل البرلمان الليبي في جلسة أكتوبر لسنة ٢٠٢١م الذي يحتوي على ٣٠ مادة.

حيث جاء في مادته الثانية يهدف هذا القانون إلى حماية التعاملات الإلكترونية للحد من وقوع الجرائم الإلكترونية وذلك بتحديد هذه الجرائم وإقرار العقوبات الرادعة لها.

حيث تضمن جرائم الدخول غير المشروع والجرائم الخاصة بحرمة الحياة والخصوصية وجرائم الأتلاف للبيانات، وجرائم الإضرار بأمن الدولة.

وقد صدر قرار من وزارة العدل الليبية رقم ٢٦ لسنة ٢٠١٦م بشأن إنشاء إدارة مكافحة أبحاث الجريمة الإلكترونية بمركز الخبرة القضائية، وذلك لتنامي وسائل تلك الجرائم ومحاولة الحد منها.

الخاتمة

يتضح من خلال عرضنا للتحول الرقمي، أنه أحدث انعكاساً على السياسة الجنائية، وتطوير القوانين وتنقيح القواعد العامة لقانون العقوبات، والقوانين الخاصة ذات الصلة، بالتطور التقني الحديث، لقد أثبتت الدراسات والتجارب على أن تقنية المعلومات والاتصالات تستطيع أن توفر للإنسان خدمات كثيرة لم يكن يعهدها من قبل، ولهذا فإن معظم الدول دأبت على توظيف هذه التقنية ووضع الخطط والاستراتيجية لتطويرها واستثمارها في جميع المجالات، وذلك من خلال إرساء مفهوم الحكومة الإلكترونية، والعمل على إسراع القوانين التي تنظم كل مسائل وأثار هذا التحول التقني.

جل التشريعات اعتدت بفكرة الكيان المادي للشيء الناتج عنه اختلاس المال المعنوي للبرمجيات والمعلومات.

حيث كان دور الاتفاقيات الدولية هام في تحديد أسس وتقسيم الجرائم المعلوماتية، مما ساعد التشريعات الوطنية في إصدار وتطوير تشريعاتها.

التوصيات:

١. العمل على تنظيم القوانين الخاصة بمقدمي الخدمة من شركات عامة وخاصة، لحماية منظومات البيانات، وتشديد العقوبات لجرائم اختراقها.

٢. النص على تجريم الدخول غير المشروع، للجهات العامة والخاصة، غير المخولة قانوناً بتلك البيانات والمنظومات التقنية، منعاً، لإساءة استعمال السلطة، وأن يتم ذلك بإذن قضائي.

قائمة المراجع

١. إبراهيم عبد الخالق، جرائم الأموال، الجزء الثاني، المكتب الفني للإصدارات القانونية، القاهرة، الطبعة الثانية، سنة ٢٠٢٠م.

٢. إيهاب علي النواب، الحكومات الإلكترونية وحتمية التحول الرقمي، شبكة النبأ للمعلومات، سنة ٢٠١٨م.

٣. بهاء المر، جرائم السوشيال ميديا، دار الأهرام، القاهرة، الطبعة الأولى، سنة ٢٠٢٢م.

٤. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، الطبعة الأولى، سنة ١٩٩٢م.

٥. جمال شحاته، قانون جرائم تقنية المعلومات، دار الأهرام، القاهرة، سنة ٢٠٢١م.

٦. حسام عامل الأهواني، الحماية الجنائية في مواجهة الحاسب الآلي، بحث مقدم في مؤتمر الكويت الأول، شبكة المعلومات، سنة ٢٠٠٠م.

٧. رزق سعد علي، انعكاسات التحول الرقمي على السياسية الجنائية المعاصرة، مجلة الدراسات القانونية، كلية الحقوق، جامعة السادات، سنة ٢٠٢١م.

٨. طارق إبراهيم الدسوقي، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، سنة ٢٠١٥م.

٩. عبد العزيز لطفي جاد الله، الجريمة السيبرانية وحماية أمن المعلومات، مؤسسة المعرفة، الإسكندرية، الطبعة الأولى، سنة ٢٠٢٢م.

١٠. عمر محمود الحوثي، الوجيز في الحماية الجنائية في جرائم تقنية المعلومات، دار النهضة العربية، القاهرة، سنة ٢٠٢١م.

١١. فرج حسن الأطرش، نحو خلق بيئة قانونية للحكومة الإلكترونية في ليبيا، مجلة كلية القانون، جامعة الجفرة، سنة ٢٠٢١م.

١٢. منظومة التشريعات الجنائية الليبية.