جامعة الأزهر
AL-AZHAR UNIVERSITY

مدى تأثير التكنولوجيا على السياسة الجنائية في ضوء قانون تقنية المعلومات

(دراسة تحليلية مقارنة)

إعداد

د/ رضا محمد عبد العزيز مخيمر

دكتوراه في القانون الجنائي

المحاضر بكلية الحقوق – جامعة طنطا

بحث مستل من الإصدار الثاني ٢/١
من العدد الثامن والثلاثين أبريل٢٠٢٣م

مدى تأثير التكنولوجيا على السياسة الجنائية في ضوء قانون تقنية المعلومات

(دراسة تحليلية مقارنة)

إعداد

د/ رضا محمد عبد العزيز مخيمر

دكتوراه في القانون الجنائي

المحاضر بكلية الحقوق – جامعة طنطا

موجز عن البحث

نحن نعيش في عصر جديد من التقدم العلمي والتقني في مجال تكنولوجيا المعلومات والاتصالات، الذي أحدث ثورة تنموية بشرية على جميع المستويات المحلية والعالمية. وقد أصبحت عملية تبادل المعلومات والمعارف أسهل وأكثر سلاسة، وتدفق المعلومات عبر وسائل الاتصال المختلفة أدى إلى تبادل الأخبار والمحادثات بحرية ويسر. ومع ذلك، فإن هذا التطور التكنولوجي خلف العديد من المخاطر والأضرار، وخاصة بسبب ضعف الرقابة عليها، مما أدى إلى ظهور نوع جديد من الجرائم المتطورة في طريقة وأسلوب ارتكابها، وصفات المجرمين وطباعهم، وهي ما يُعرف بجرائم التقنية المعلوماتية، وتمثل تهديدًا مباشرًا وواضحًا للأمن والاستقرار المحلي والعالمي، وتشكل عائقًا أمام التنمية الاقتصادية والأمنية.

وبالتالي، سعت العديد من الدول إلى تطوير نظمها التشريعية بإدخال نصوص وتشريعات عقابية وإجرائية تتوافق مع ظاهرة الإجرام التقني الحديثة، ومن هذه التشريعات ما كان موفقًا ومنها ما أصابه بعض الخلل والقصور، ولذلك فإنه يجب دراسة وتحليل هذه التشريعات بشكل مقارن لتحسينها وتطويرها.

الكلمات المفتاحية: التكنولوجيا ، المواجهة التشريعية. قواعد الإختصاص، القانون المطبق، الدليل الجنائي الرقمي.

The Impact Of Technology On Criminal Policy
In Light Of The Information Technology Law (Comparative Analytical Study)

Reda Mohamed Abdel Aziz Mukhaimer
Department of Criminal Law، Faculty of Law، Tanta University، Egypt
E-mail : Rda475979@gmail.com

Abstract :

We are living in a new era of scientific and technological advancement in the field of information and communication technology، which has brought about a human development revolution at all local and global levels. The process of exchanging information and knowledge has become easier and smoother، and the flow of information through various communication channels has led to the free and easy exchange of news and conversations. However، this technological development has created many risks and damages، particularly due to the weak control over it، resulting in the emergence of a new type of advanced crimes in terms of the method and style of their commission، the characteristics of the criminals، and what is known as cybercrime. It represents a direct and clear threat to local and global security and stability and poses an obstacle to economic and security development. Therefore، many countries have sought to develop their legislative systems by introducing punitive and procedural texts and legislation that are compatible with the modern cybercrime phenomenon. Some of these legislations have been successful، while others have suffered from some flaws and shortcomings. Therefore، studying and analyzing these legislations comparatively is necessary to improve and develop them.

Keywords: Technology، Legislative Confrontation، Jurisdiction Rules، Applied Law، Digital Criminal Evidence.

مقدمة

التكنولوجيا الحديثة هي تحول تاريخي وثقافي يسير جنبًا إلى جنب مع التقدم العلمي لتبسيط الإجراءات وجعل الحياة الاجتماعية أفضل وأسهل. وينعكس هذا الجانب الإيجابي في القانون الجنائي ويصبح أهم أداة للسياسة الجنائية الحديثة لتحقيق أهدافها. ومع ذلك ، فإن لهذه التكنولوجيا أيضًا جانبًا سلبيًا ، مما يؤدي إلى التطوير النوعي للجرائم الرقمية أو المعلوماتية وانتهاكات الحقوق الفردية والسيادة الوطنية(١). فمن حيث التشريع، يسمح لجميع الدساتير والمعاهدات والاتفاقيات الدولية والوطنية للإنسان إستخدام وسائل تكنولوجيا المعلومات استخدامًا كاملاً وبحرية وتبادل البيانات والمعلومات مع وسائل التواصل الاجتماعي إلا أن هذه الحرية لاينبغي أن تجعل من الانترنت ووسائل التقنية الحديثة ، بيئة بلا قواعد ونصوص قانونية التي تحكمها وتنظمها(٢). وإزاء ذلك حرص المشرع المصري على تطوير نظم المواجهة التشريعية لجرائم تقنية المعلومات(٣)، بإدخال نصوص

---

(١) د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الألات الحديثة، القاهرة، ١٩٩٢، ص٤٥.

(٢) انظر: قرار محكمة استئناف أوبونتو في أحد أهم القرارات الصادرة في ٢ فبراير ٢٠٠٥ .

Ch. Caron: ، Comm. 35، 2 février2005: Comm.Com. Electr. 2005، 6e ch.،TGI Pontoise " l'outil exceptionnel de communication et d'échange que représente le réseau internet ne saurait être lieu de liberté où les ، c'est-à-dire un univers،en tout état de cause une zone de non droit règles juridiques élémentaires ne s'appliquent pas ".

(٣) د/ أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الألي، دار النهضة العربية، القاهرة، ١٩٨٢،

تشريعية عقابية وإجرائية تتلائم مع ظاهرة الإجرام التقني الحديث بإصدار القانون رقم ١٧٥ لعام ٢٠١٨م، ولائحته التنفيذية رقم ١٦٩٩ لعام ٢٠٢٠م، بشأن مكافحة جرائم تقنية المعلومات. فالمشرع المصري قام قبل إصدار هذا القانون بإصدار بعض القوانين الخاصة بالبيئة الرقمية أو المعلوماتية مثل، القانون ١٤٣ لعام ١٩٩٤م بشأن الأحوال المدنية والذي يرتبط بحماية البيانات والوثائق الرسمية، ويعد هذا القانون أول التشريعات الخاصة التى أصدرها المشرع المصري بشأن حماية المعلومات المسجلة إلكترونياً(١). أما فيما يتعلق بالتشريعات العربية المقارنة ، فقد قامت دولة الإمارات العربية المتحدة بإصدار القانون الاتحادي رقم ٥ لعام ٢٠١٢ م وتعديلاته لمكافحة جرائم التقنية المعلوماتي(٢)، فمن ناحية أخرى تلعب الجوانب التشريعية والقانونية دورًا مهمًا في إطار تقنية المعلومات حيث لا بد من وجود تشريعات تنظم توافر واستخدام الخدمات الحكومية حيث تكمن أهمية سن التشريعات والقوانين المتعلقة بالمعاملات الإلكترونية في كل من التقليدية

ص٣٢١.

(١) د/ عمر محمد سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي ، المراقبة الالكترونية والتحقيق الجنائي عن بعد، دار النهضة العربية ، القاهرة، ٢٠١٣م، ص٢٧.

(٢) انظر: القانون رقم ٥ لسنة ٢٠١٢ م والمعدل بموجب المرسوم بقانون الاتحادي رقم ٢لسنة ٢٠١٨ م ، الجريدة الرسمية ، السنة الثانية والأربعون ، العدد ٤٥٠ بشأن مكافحة جرائم التقنية المعلوماتي الإماراتي.

أولاً: أهمية البحث

يتجلى أهمية هذا البحث في محاولة الباحث لتسليط الضوء على ظاهرة الإجرام التقني كظاهرة حديثة تتطلب دراسة وبحثًا أعمق، وذلك نظرًا لظهور هذه الجرائم بشكل واضح ومنتشر في العديد من المجالات وعلى جميع المستويات.

وتأتي أهمية هذه الدراسة في تقديم دراسة عامة تحليلية لنصوص قانون مكافحة جرائم تقنية المعلومات المصري الصادر بالرقم ١٧٥ لعام ٢٠١٨ م ولائحته التنفيذية من الناحيتين الموضوعية والإجرائية. وقد اعتمد الباحث في هذه الدراسة على الإسلوب التحليلي المقارن، حيث قام بمقارنة بعض النصوص والتشريعات العربية والأوروبية بهدف التحقق من كفاءة هذه النصوص في مكافحة ظاهرة الإجرام التقني، والتعرف على أهم الضوابط وسبل وآليات التعاون الدولي في مجال مكافحة هذه الجرائم. ويأتي ذلك بغية تحسين صياغة النص وتعزيز فاعليته في مكافحة هذه الظاهرة المتزايدة

ثانياً : سبب إختيار موضوع البحث

تأثير التكنولوجيا على السياسة الجنائية هو موضوع مهم ومثير للاهتمام، ويمكن أن يكون موضوع بحث جيد للعديد من الأسباب. و يعد موضوعـًا حديثـًا ومتغيراً باستمرار، حيث تتطور التكنولوجيا بسرعة كبيرة وتتغير السياسات الجنائية بشكل مستمر لمواكبة هذا التطور. كما أن قانون تقنية المعلومات هو قانون هام يتعلق بحماية البيانات والمعلومات الإلكترونية، وله تأثير كبير على السياسة الجنائية

فيما يتعلق بجرائم الإنترنت والجرائم التقنية الأخرى. ويمكن أن يساهم هذا الموضوع في فهم أفضل للتحديات التي تواجه الدول والمجتمعات في ضوء التطور التكنولوجي السريع، وكيفية مواجهة هذه التحديات من خلال السياسة الجنائية.

وأخيراً، يمكن أن يساعد هذا الموضوع في تطوير السياسات الجنائية والقانونية المتعلقة بالتكنولوجيا وحماية البيانات والمعلومات الإلكترونية، ويمكن أن يساهم في تحسين الأمن الإلكتروني والحفاظ على حقوق المستخدمين والمجتمعات على الإنترنت.

ثالثاً: نطاق البحث

تعرض القانون رقم ١٧٥ لعام ٢٠١٨م ولائحته التنفيذية رقم ١٦٩٩ لعام ٢٠٢٠م بشأن مكافحة جرائم تقنية المعلومات، للمواجهة الجنائية لجرائم تقنية المعلومات ليس المحلى فقط بل العابر للحدود الذي لا يمكن حصره في نوع أو مكان محدد للجرائم الرقمية. كما إشتمل على بيان الجرائم والعقوبات التى تترتب على مخالفة أحكامه، وإمكانية التصالح في تلك الجرائم، إلا أن كل التسميات لجرائم تكنولوجيا التحول الرقمي يحددونها في جرائم الحاسب الآلي واستعماله فقط. وعلى ذلك يتحدد نطاق هذه البحث بتناول أولا: مفهوم التكنولوجيا ، ثانيا: مفهوم السياسة الجنائية، ثالثا : الفرق بين التكنولوجيا والسياسة الجنائية، في المبحث الأول؛ ثم نتعرض لأبرز ملامح تطوير السياسة التشريعية في ضوء أحكام قانون مكافحة جرائم تقنية المعلومات أولا: الجهود التشريعية

لمواجهة جرائم تقنية المعلومات. ثانيا: تطور قواعد الاختصاص والقانون واجب التطبيق . ثالثا: حجية الدليل الرقمي في الإثبات الجنائي. في المبحث الثاني؛ ونحن إذ نتناول البحث في تسليط الضوء على مدى تأثير التكنولوجيا على السياسة الجنائية في ضوء قانون مكافحة جرائم تقنية المعلومات .

رابعاً: منهج البحث

المنهجية التي اخترناها لفحص موضوع الدراسة هي النهج التحليلي المقارن .لكي تتوافق طبيعة البحث وأهدافه في المقام الأول مع استقراء وتحليل الأحكام . المدرجة في اختصاص القانون رقم ١٧٥ لعام ٢٠١٨ م بشأن الجرائم التكنولوجية في مصر وفقًا لاحتياجات وأهداف البحث ، اخترنا بعض التشريعات العربية والأوربية للمقارنة والتحليل، مع إبراز القيود الخاصة بكل منها من خلال تقديم سلسلة من الاقتراحات المهمة ، من الممكن معالجة العيوب الموجودة ومعالجتها بشكل فعال.

خامساً: أهداف البحث

تركز هذه الدراسة على مقارنة وتحليل الأحكام المنصوص عليها في قانون مكافحة جرائم التكنولوجيا. والهدف هو تحديد اللوائح المتعلقة بتنفيذ المعلومات من المنظورين الموضوعي والإجرائي . والفوائد الواردة في التشريع المصري والقيود التي تنتقص من فعاليته .عند مقارنتها بالنصوص والقوانين العربية والأوربية المتعلقة بنفس الموضوع ، يتضح أن هناك بعض الاختلافات والتشابهات في

محتواها. وتقييم فعالية وكفاية القوانين المتعلقة بالمخالفات الفنية ومدى فعاليتها .

سادساً: إشكالية البحث

مشكلة هذه الدراسة أنه بسبب حداثة جرائم تقنية المعلومات هذه ، وحقيقة أن بعض الدول تطبق قوانين تقليدية لا تتناسب مع خطورتها ، ولا يوجد نص تشريعي للتعامل مع هذه الجرائم والنصوص القانونية التي تستند إليها. يعتمد التفكير في مكافحة جرائم التكنولوجيا. بخلاف المشرع المصري والتشريعات المقارنة بسن قانون مكافحة جرائم تقنية المعلومات مشكلة هذا البحث هي أيضا السؤال التالي:

- ما هي مفاهيم التكنولوجيا والسياسة الجنائية؟
- ما هي ملامح تطوير السياسة التشريعية في قانون مكافحة جرائم تقنية المعلومات؟
- ما هي قواعد الاختصاص القضائي والقانون واجب التطبيق في جرائم تقنية المعلومات؟
- ما هي حجية الدليل الجنائي الإلكتروني؟

سابعاً : خطة البحث

من خلال هذه البحث نسلط الضوء على مدى تأثير التكنولوجيا على السياسة الجنائية وبعض ملامح تطوير السياسة التشريعية لمكافحة جرائم تقنية المعلومات وفقا للقانون رقم ١٧٥ لعام ٢٠١٨ م ولائحته التنفيذية رقم ١٦٩٩ لعام ٢٠٢٠م . وذلك من خلال مبحثين:

المبحث الاول : الأحكام العامة للتكنولوجيا والسياسة الجنائية.

المطلب الأول: مفهوم التكنولوجيا.

المطلب الثاني: مفهوم السياسة الجنائية.

المطلب الثالث: الفرق بين التكنولوجيا والسياسة الجنائية.

المبحث الثاني: ملامح تطوير السياسة التشريعية في ضوء قانون تقنية المعلومات.

المطلب الأول: المواجهة التشريعية لجرائم تقنية المعلومات.

المطلب الثاني: تطور قواعد الإختصاص والقانون الواجب التطبيق.

المطلب الثالث:حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية.

الخاتمة والتوصيات.

المبحث الاول
الأحكام العامة للتكنولوجيا والسياسة الجنائية

تمهيد و تقسيم:

التكنولوجيا تشير إلى الانتقال من الأنظمة التقليدية إلى الأنظمة الرقمية القائمة على تقنيات المعلومات والاتصالات في جميع مجالات العمل(١). وتتطلب هذه الانتقالات التشريع والتنظيم اللازم لتوافر واستخدام التقنية بطريقة قانونية وآمنة(٢). ومن المهم التأكيد على أن الجوانب التشريعية والقانونية تلعب دورًا مهمًا في الإطار الفني، حيث لا يمكن تحقيق التقدم التكنولوجي بدون تنظيم وتوجيه الاستخدام القانوني للتقنية. ويجب أن يتم تقديم التشريعات والقوانين اللازمة لتنظيم وتوجيه استخدام تقنية المعلومات، نظرًا لأن التقنية الرقمية تختلف عن الخدمات التقليدية، وتحتاج إلى قوانين وتشريعات خاصة بها. ويجب أن يكون هناك تنظيمات قانونية متعلقة بالمعاملات الإلكترونية في البيئة التقنية، ويجب أن تكون هذه التنظيمات واضحة وشاملة لتحقيق الأمان والحماية للمستخدمين(٣). من بين التقنيات التي غيرت العالم وأحدثت تغييرات جذرية في السياسة الجنائية، تشمل أجهزة الكمبيوتر

(١) د/ هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية ، القاهرة، ١٩٩٩، ص١٠٩.

(٢) د/ هدى حامد قشقوش، جرائم الحاسب الآلي الإلكترونيةفي التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢، ص١٠.

(٣) د/ جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١، ص٦.

والذكاء الاصطناعي والحوسبة. ويمثل التحول الرقمي والمفاهيم الحديثة الأخرى مثل التحليل الجنائي الرقمي والتحقق من الهوية الرقمية وغيرها، أدوات مهمة تستخدم في مكافحة الجريمة وتحقيق العدالة.

وبالتالي، فإن العمل المتزامن بين التكنولوجيا والتشريعات القانونية يساعد في تحقيق الأهداف المشتركة والتي ترتكز على الأمن والحماية والعدالة في جميع المجالات، بما في ذلك المجال الجنائي(١).

سوف نتناول هذا المبحث من خلال ثلاثة مطالب على النحو التالي:

المطلب الأول: مفهوم التكنولوجيا.

المطلب الثاني: مفهوم السياسة الجنائية.

المطلب الثالث: الفرق بين التكنولوجيا والسياسة الجنائية.

المطلب الأول : مفهوم التكنولوجيا

تشير التكنولوجيا إلى الانتقال من الأنظمة التقليدية إلى الأنظمة الرقمية القائمة على تقنيات المعلومات والاتصالات في جميع مجالات العمل من خلال سلسلة من المتطلبات التشريعية والقانونية(٢).

أولاً- تعريف التكنولوجيا: التكنولوجيا هي الاستخدام العملي للمعرفة

(١) د/ عمر محمد سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي ، المراقبة الالكترونية والتحقيق الجنائي عن بعد، دار النهضة العربية ، القاهرة، ٢٠١٣م، ص٢٧.

(٢) د/ هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية ، القاهرة، ١٩٩٩، ص١٠٩.

والأدوات والموارد لتلبية الاحتياجات والرغبات البشرية(١). وتشمل التكنولوجيا المختلفة مجموعة واسعة من المجالات مثل الحوسبة والاتصالات والطب والطاقة والنقل وغيرها، وتتطور باستمرار لتلبية الاحتياجات الجديدة وحل المشكلات الحالية. وتؤثر التكنولوجيا بشكل كبير على الحياة اليومية للناس وعلى التطور الاقتصادي والاجتماعي والثقافي للمجتمعات(٢).

ثانيًا- تعريف التحول الرقمي: استخدام تكنولوجيا الكمبيوتر والإنترنت في عملية خلق قيمة عملية أكثر كفاءة وفعالية ، والإشارة على نطاق واسع إلى التغييرات التي تحدثها التقنيات الجديدة ، وكيفية العمل والتفاعل بشكل عام(٣)، ويتم التعامل مع التحول الرقمي بشكل مكثف مع المفاهيم الحديثة(٤)، ومن ثم تكمن الفكرة الرئيسية لاستراتيجية الأعمال الرقمية في كيفية فهم تكنولوجيا المعلومات كشرط أساسي للابتكار وسرعة التنفيذ وسهولة.(٥) كما يُعرَّف التحول

(١) د/ فضيل دليو، تكنولوجيا الإعلام والإتصال الجديدة بعض تطبيقاتها التقنية، دار هومة للطباعة والنشر، الجزائر، ٢٠١٢، ص٢٠.

(٢) د/ غيث محمد عاطف، قاموس علم الاجتماع، دار المعرفة الجامعية، الإسكندرية، ١٩٩٩، ص٢٦٥.

(٣) د/ سيف بن عبد الله الجبري، المكتبة الرقمية ودورها في بناء وتطوير مجتمع المعرفة التحديات الاجتماعية والثقافية واللغوية في العالم حاضراً ومستقبلاً، المؤتمر العلمي لكلية الأداب والعلوم الاجتماعية في الفترة ٢-٤ ديسمبر، ٢٠٠٧، ص١٥.

(4)Hinings،B.،Gegenhuber،T.،Greenwood، R.،2018.Digital lnnovation and Transformation:An lnstitutional Perspective. Lnformation and Oranization28،51-66.

(٥) انظر: المؤتمر الدولي لمعهد التخطيط القومي" اقتصاد المعرفة والتنمية المستدامة" الورقة المفاهيمية ،

الرقمي عمومًا على أنه: عملية إنهاء الخدمات، وإنشاء وتقديم قيمة حديثة عن طريق التكنولوجيا الحديثة ؛ أو تطبيق التكنولوجيا، من خلال تطبيق تكنولوجيا الذكاء الاصطناعي ومفردات العالم الافتراضي، وإحداث تغييرات شاملة في الخدمات والشركات (١).

ثالثًا- فوائد التكنولوجيا:

تتمثل أبرز الفوائد للتكنولوجيا في كل من الأتي(٢):

- تخفيض التكاليف.
- تحسين تكنولوجيا الأعمال القانونية والقضائية والاعتماد على التكنولوجيا الرقمية يعني توفير التكلفة لكل المتقاضين، كما أنه يعمل على تحسين الكفاءة وينظمها.
- استراتيجية محسنة للمتقاضين.
- تحليل البيانات القانونية.
- القضاء على الاعتماد على أنظمة تكنولوجيا المعلومات العادية البطيئة، لتصبح

القاهرة ، ٢٠٢١م، ص٥.

(١) د/ مصطفي أحمد أمين، التحول الرقمي في الجامعات المصرية، كمطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد١٩، ٢٠١٨، ص٢١.

(٢) د/ مصطفي أحمد أمين، التحول الرقمي في الجامعات المصرية، كمطلب لتحقيق مجتمع المعرفة، المرجع السابق، ص١٩.

منظومة القانون والقضاء أكثر ذكاءً.

رابعـًا- متطلبات التكنولوجيا:

ثورة التكنولوجيا ثورة لا نهاية لها، فيوميـًا يبدع العلماء بإبتكار مستجدات تكنولوجيا تيسر حياة الإنسان(١)، ولكن بالمقابل وفي الجانب التنظيمي هناك متطلبات لتطبيق التكنولوجيا وهي(٢):

تغيير أسلوب التعليم للعنصر البشري القضائي والقانوني للحصول على مهارات حديثة وترشيد مستقبلي حتى يستطيعوا من تحقيق الازدهار في المجتمع و البيئة الرقمية القضائية.

اقامة البنية التحتية للاتصالات الرقمية لمنظومة القانون والقضاء وصيانتها وإمكانية الوصول إليها وضمان إدارتها، وتحقيق التكافؤ بين تكاليف وجودة الخدمات القضائية.

تحقيق الشفافية للمواطنين داخل منظومة القانون والقضاء وضمان متطلبات الاستقلالية، وتعزيز الثقة و حماية البيانات الرقمية.

---

(1) Liere-Netheler،K.،Packmohr،S.،Vogelsang،K.،2018،Drivers of digital transformation in manufacturing. Ln: Hawaii International Conferece on System Sciences،Waikoloa Beach، HI،pp.3926-3930.

(٢) د / محمد موسي على شحاته، انعكاسات تفعيل آليات التحول الرقمي في ضوء مبادرات الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية ، بحث منشور بمجلة الدراسات المعاصرة، العدد ٩، ٢٠٢٠، ص٢٠٦.

اتاحة الوصول إلى الخدمات داخل منظومة القانون والقضاء من خلال تحسين الخدمة العامة وإرساء ضوابط وآليات وجودة الخدمات الرقمية.

تحسين الإطار التنظيمي لمنظومة القانون والقضاء وتنفيذ نماذج مبتكرة وأعمال حديثة المقدمة للمجتمع.

المطلب الثاني : مفهوم السياسة الجنائية

أولاً- تعرف السياسة الجناية لغويًا: بأنها مجموعة القواعد والإجراءات التي تحدد الجرائم المعاقب عليها وأنواع العقوبات المناسبة لكل جريمة. وبشكل أكثر تحديدًا، فإن السياسة الجنائية تشمل القوانين واللوائح التي تحدد السلوكيات التي تعتبر جرائم، وكذلك الإجراءات القانونية والإدارية التي تتخذها الحكومة لمكافحة الجريمة ومعاقبة المتسببين فيها. وتتضمن السياسة الجنائية أيضًا العديد من الجوانب الأخرى مثل التدابير الوقائية والبرامج الإصلاحية التي تهدف إلى تحسين النظام القضائي والتقليل من معدلات الجريمة(١).

ثانيـًا- تعريف السياسة الجنائية اصطلاحـًا: بأنها المجموعة المنظمة من الخطط والإجراءات التي تقوم بها الحكومة أو السلطة المسؤولة عن تطبيق القانون للتعامل مع الجرائم والمخالفات في المجتمع. وتهدف السياسة الجنائية إلى تحديد السلوكيات التي تعد مخالفة للقانون وتحديد العقوبات التي يجب فرضها على

(١) د/ أحمد فتحى سرور ، الوسيط فى قانون العقوبات. القسم العام، دار النهضة العربية، القاهرة، ٢٠١٥، ص ٢٥ .

المخالفين. وتشمل السياسة الجنائية أيضًا الإجراءات التي تتخذها الحكومة أو السلطة المسؤولة عن تطبيق القانون للحد من الجرائم والمخالفات والحفاظ على النظام والأمن العام. وتعتمد السياسة الجنائية على القوانين واللوائح والسياسات الأخرى التي يتم وضعها من قبل السلطات التشريعية والتنفيذية. ويعد العالم الألماني، دونديه دي فابر بأن السياسة الجنائية : مجموعة الأساليب التي تخصصها الدولة للمحاسبة على نوع الجريمة، ولقد انتقد هذا التعريف من جانب الغرض من السياسة الجنائية بالعقوبة المترتبة كأثر للجريمة المرتكبة، وهذا ما يتنافي مع وظيفة السياسة الجنائية المتمثلة بالإصلاح الشامل للقانون الجنائي(١).

ثالثًا- تعريف السياسة الجنائية قانونا :بأنها الإطار الذي تعتمده الدولة لتحديد الجرائم والعقوبات المنصوص عليها في القانون، وكيفية تنفيذها(٢).وتتضمن السياسة الجنائية عدة عناصر منها: تعريف الجرائم وتحديدها، وتحديد العقوبات والإجراءات التي يتم اتخاذها لتنفيذها، وتحديد السلطات المختصة بتنفيذ القانون الجنائي، وتحديد الحقوق والضمانات التي يتمتع بها المتهمون والمتهمات، وتحديد الإجراءات القانونية التي يجب اتباعها في مراجعة الأحكام الجنائية

(١) د/ محمد عبد اللطيف فرج، السياسة الجنائية المعاصرة والإتجاهات تطوير القانون الجنائي ودعم التعاون الدولي، الطبعة الأولي ، مطابع الشرطة ، القاهرة ، ٢٠١٣، ص١٥.

(٢) د/ أحمد فتحى سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، ٢٠١٥ م ، ص١٩.

والاستئناف منها، وتحديد العوامل التي يجب مراعاتها في تطبيق القانون الجنائي، مثل العمر والنوع والحالة الاجتماعية والثقافية للمتهمين والمتهمات. وتهدف السياسة الجنائية إلى تحقيق العدالة الجنائية وحماية المجتمع من الجرائم والتهديدات الأمنية(١).

وتشتمل السياسة الجنائية في التشريع المصري على المبادئ والإجراءات التي يتم اتباعها لتحقيق العدالة الجنائية وحماية المجتمع من الجرائم. وتشمل هذه السياسة العديد من الجوانب المختلفة، بما في ذلك:

١- تحديد الجرائم وتصنيفها وتحديد العقوبات الواجبة على المرتكبين.

٢- توفير الإجراءات القانونية والإدارية اللازمة للتحقيق في الجرائم ومحاكمة المتهمين.

٣- تطوير النظام القضائي وتحسين تقنيات التحقيق والتدخل الجنائي.

٤- تعزيز التعاون الدولي في مجال مكافحة الجريمة والتعاون مع الجهات الأمنية الدولية.

ويتم تطبيق هذه السياسة الجنائية من خلال عدة مؤسسات قضائية وأمنية في مصر، بما في ذلك النيابة العامة والمحاكم والشرطة والهيئات الأمنية الأخرى. وتسعى مصر دائمًا إلى تحسين سياساتها الجنائية وتطويرها لتحقيق العدالة الجنائية

(١) د/ مصطفى العوجي، دروس العلم الجنائي، مؤسسة نوفل، بيروت - لبنان ، ١٩٨٠، ص ١٢٥.

وحماية المجتمع. وتلتزم مصر أيضًا بالمعاهدات الدولية والاتفاقيات المتعلقة بمكافحة الجرائم وتعزيز التعاون الدولي في هذا المجال.كما تشتمل السياسة الجنائية في التشريع الإماراتي على المبادئ والإجراءات التي يتم اتباعها لتحقيق العدالة الجنائية وحماية المجتمع من الجرائم. وتشمل هذه السياسة العديد من الجوانب المختلفة، بما في ذلك:

١- تحديد الجرائم وتصنيفها وتحديد العقوبات الواجبة على المرتكبين.

٢- توفير الإجراءات القانونية والإدارية اللازمة للتحقيق في الجرائم ومحاكمة المتهمين.

٣- تطوير النظام القضائي وتحسين تقنيات التحقيق والتدخل الجنائي.

٤- تعزيز التعاون الدولي في مجال مكافحة الجريمة والتعاون مع الجهات الأمنية الدولية.

ويتم تطبيق هذه السياسة الجنائية من خلال عدة مؤسسات قضائية وأمنية في الإمارات، بما في ذلك النيابة العامة والمحاكم والشرطة والهيئات الأمنية الأخرى. وتسعى الإمارات دائمًا إلى تحسين سياساتها الجنائية وتطويرها لتحقيق العدالة الجنائية وحماية المجتمع.

تعقيب:

يجب أن تواكب القوانين الجنائية التطورات التكنولوجية(١). حيث سنت معظم دول العالم القانون الجنائي في القرنين التاسع عشر والعشرين، وتحولت الأيديولوجيات والابتكارات الاجتماعية التي سادت في القرن الماضي لتشهد في القرن الحادي والعشرين(٢). كما تبين أن هناك جريمة حديثة تعرف بالجريمة الرقمية أو "المعلوماتية"(٣). ارتبطت بازدهار كبير في مجال التكنولوجيا الحديثة. مع التقدم المذهل في استخدام شبكة المعلومات الدولية "الإنترنت"، وكانت الجريمة الإلكترونية بأشكالها المختلفة (٤) معروفة سابقًا في شكل تهديدات لأمن المعلومات من خلال جرائم لا ينظمها القانون الجنائي ، كما هو الحال في المجال واسع الانتشار لمعالجة المعلومات واسترجاعها ونقلها وتخزينها بغرض تغييرها أو تعديلها أو إتلافها، أصبح أرضًا خصبة للجرائم الرقمية(٥) .

المطلب الثالث : الفرق بين التكنولوجيا والسياسة الجنائية

التكنولوجيا والسياسة الجنائية هما مجالان مختلفان، ولكن يمكن أن يكون لهما تأثير متبادل. والتكنولوجيا تشير إلى الأدوات والأجهزة والبرمجيات الحديثة التي

---

(١) د/ محمد حماد هيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة ، عمان، الطبعة الأولي، ٢٠٠٤، ص٥٥.

(٢) د/ أحمد الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية ، جامعة مؤتة، الأردن، المجلد الأول، العدد٣، ٢٠٠٩، ص١٣٠ .

(3)MASCALA Corinne،"crimialite et contrat electronique"،IN:Le contrat électronique،Travaux de L'association CAPITANT Henri، jornées national،Paris،2000،P120.

(4) TOM Forester،Essential problémes to High-tech Society First MIT Prés édition، Cambridge،Massachusetts،1989،P.100.

(٥) د/ محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، ٢٠٠٤، ص٥٠.

تستخدم لتحسين الأداء وتسهيل المهام في مختلف المجالات. وتشمل التكنولوجيا مثلًا الحوسبة السحابية والذكاء الاصطناعي والإنترنت والهواتف الذكية والأجهزة اللوحية وغيرها(١).

أما السياسة الجنائية فهي المجموعة من السياسات والتشريعات والإجراءات التي تهدف إلى تنظيم النظام الجنائي وفرض القانون والعدالة في المجتمع. وتشمل السياسة الجنائية مثلًا قوانين الجرائم والعقوبات والإجراءات القانونية والإجراءات الخاصة بتنفيذ العقوبات(٢). على الرغم من أن التكنولوجيا والسياسة الجنائية هما مجالان مختلفان، إلا أن استخدام التكنولوجيا في تنفيذ السياسة الجنائية يمكن أن يؤدي إلى تحسين الأداء وتسهيل المهام في المجال الجنائي. على سبيل المثال، يمكن استخدام التكنولوجيا في تحليل البيانات والأدلة الرقمية لتحديد الجرائم والمتهمين، وتحسين الأمن الإلكتروني وحماية البيانات الحساسة والخصوصية. وباستخدام التكنولوجيا في السياسة الجنائية، يمكن تحسين العمليات القانونية وتسريعها، كما يمكن أيضـًا تحسين تحليل البيانات والأدلة الرقمية لتحديد الجرائم والمتهمين، وتحسين عمليات البحث والتحقيق والتحقق من الهوية. ويمكن أيضـًا

---

(١) د/ محمد سامي الشوا، ثورة المعلومات وإنعكاستها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٥، ص٢٥.

(٢) د/ هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية ، دار النهضة العربية، ٢٠١٢، ص٥٠.

استخدام التكنولوجيا في تعزيز الأمن الإلكتروني وحماية البيانات الحساسة والخصوصية، خاصة في ظل انتشار الجرائم الإلكترونية والاختراقات السيبرانية. ومن الأمثلة الواضحة لتأثير التكنولوجيا على السياسة الجنائية، يمكن الإشارة إلى استخدام أنظمة التعرف على الوجوه والبصمات الإلكترونية في التحقق من هوية المشتبه بهم والمتهمين، واستخدام البرمجيات الحديثة لتحليل البيانات والأدلة الرقمية للكشف عن الجرائم والمخالفات، واستخدام الروبوتات والأجهزة الذكية في تعزيز الأمن ومراقبة الأنشطة الجنائية. ومع ذلك، يجب ملاحظة أن استخدام التكنولوجيا في السياسة الجنائية يمكن أن يواجه بعض التحديات والمخاطر، مثلًا إمكانية انتهاك الخصوصية والحقوق الشخصية، وتعرض الأجهزة والبرمجيات للاختراق والاستغلال السيبراني. لذلك، يجب أن يتم استخدام التكنولوجيا في السياسة الجنائية بشكل مسؤول وفقًا للقوانين والأنظمة القانونية المعمول بها، وتحسين الأمن الإلكتروني لضمان حماية البيانات والخصوصية والحقوق الأساسية للأفراد[١].

(١) د/ عمر إبراهيم الوقاد، الحماية الجنائية للمعلوماتية، دار النهضة العربية، القاهرة، ١٩٩٩، ص٦٠.

المبحث الثاني
ملامح تطوير السياسة التشريعية في ضوء قانون تقنية المعلومات

تمهيد وتقسيم:

مع ظهور وسائل تقنية المعلومات التي تتمتع بميزاتها المتعددة والعابرة للحدود الجغرافية والسياسية والثقافية والدينية، أصبحت الحدود الدولية والسيادة الوطنية معرضة للانتهاك والمراقبة، وزادت حالات الاختراق الأمني من خلال عمليات التجسس والإرهاب الإلكتروني والاقتصادي وبث الشائعات والأخبار الكاذبة لإحداث البلبلة بين أفراد المجتمع. ولذلك، يصبح من الضروري الإسراع في إيجاد مواجهة تشريعية تتناسب وتلاءم هذا التطور التقني وما يصاحبه من تطور في عالم الجريمة. ولا يمكن الخوض في دراسة هذه المشكلات وسبل مواجهتها تشريعياً قبل إلقاء نظرة عامة حول قانون مكافحة جرائم تقنية المعلومات والتعرض لأهم الأحكام العامة للقانون فيما يتعلق بجرائم تقنية المعلومات، وعرض أهم الجهود التشريعية المبذولة في هذا الشأن التقني، ثم بيان أهم الضوابط المتعلقة بالتعاون الدولي. ويتعين إعادة صياغة النص بما يتناسب مع التحديات الحديثة التي يواجهها العالم في مجال مكافحة جرائم تقنية المعلومات، وتعزيز فعالية التشريعات والضوابط المتعلقة بذلك، وتعزيز التعاون الدولي لمواجهة هذه الجرائم[1].

(١) د/ عادل يحي قرني، التحقيق والمحاكمة الجنائية عن بعد، دراسة تحليلية تأصيلية لتقنية ال video conference في المجال الجنائي، الطبعة الأولي، دار النهضة العربية ، القاهرة، ٢٠٠٦، ص٥٥.

سوف نتناول هذا المبحث من خلال ثلاثة مطالب على النحو التالي:

المطلب الأول : المواجهة التشريعية لجرائم تقنية المعلومات.

المطلب الثاني: تطور قواعد الاختصاص والقانون الواجب التطبيق

المطلب الثالث: حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية.

المطلب الأول
المواجهة التشريعية لجرائم تقنية المعلومات

تتميز جرائم التقنية بتنوعها وتعقيدها، حيث تشكل خطرًا على الصعيدين الاقتصادي والقانوني، وتنطوي على انتهاك حقوق المجتمع والأفراد. ولذلك، تتطلب مكافحة هذه الجرائم تبني المزيد من التشريعات والقوانين العقابية والإجرائية التي تتناسب مع خطورتها، وتحديد الضوابط اللازمة لمواجهتها، وخلق آليات قانونية للحماية من أخطارها(١).

أولا- تعريف تقنية المعلومات: عرف المشرع المصري تقنية المعلومات في نص المادة الأولي من قانون تقنية المعلومات على أنها: مجموعة من الوسائل المترابطة أو المستقلة .هذا النظام مترابط ، ويعمل كوسيلة للتخزين والاسترجاع والترتيب والتنظيم والمعالجة والتطوير والتبادل .أي نوع من المعلومات أو البيانات مع الوسائط والطرق المستخدمة لنقلها سواء كانت سلكية أو لاسلكية. (٢) كما عرفتها

(١) انظر: استراتيجية مصر الرقمية: منشور على الموقع الالكتروني .mcit.gov.eg.Technology

(٢) انظر: المادة الأولي من القانون رقم ١٧٥ لسنة ٢٠١٨، ولائحته التنفيذية ، الجريدة الرسمية ، العدد ٣٢

الإتفاقية العربية لمكافحة جرائم تقنية المعلومات: في نص المادة الثانية من الاتفاقية بأنها " أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة، تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفقاً للأوامر والتعليمات المخزنة بها، ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أوشبكة" [1]. كما عرف المشرع الإماراتي تقنية المعلومات في نص المادة الأولي من المرسوم الإماراتي كأداة جهاز إلكتروني أو مغناطيسي أو بصري أو كهروكيميائي أو أي جهاز آخر للمعالجة أداء البيانات الإلكترونية والعمليات المنطقية والحسابية أو وظائف الذاكرة ، يتضمن أي أجهزة متصلة أو متصلة مباشرة تسمح لهذا الجهاز بالتخزين المعلومات الإلكترونية أو تسليمها للآخرين[2]. وفي سبيل تحقيق ذلك مرت العملية التشريعية في مجال مكافحة الجريمة التقنية بالعديد من الجهود المتطورة على المستويين الأوروبي والعربي، ووضع نصوص عقابية وإجرائية رادعة.

ثانياً- الجهود التشريعية الأوروبية في مجال مكافحة جرائم تقنية المعلومات.

مكرر ، بشأن قانون مكافحة جرائم تقنية المعلومات المصري.

(١) انظر: المادة الثانية من الاتفاقية العربية بموجب قرار رئيس الجمهورية رقم ٢٧٦ لسنة ٢٠١٤ المكافحة جرائم تقنية المعلومات.

(٢) انظر: المادة الأولي من المرسوم الاتحادي رقم ٥ لسنة ٢٠١٢ وتعديلاته، بالجريدة الرسمية، العدد ٤٥٠، السنة الثانية والأربعون، بشأن قانون مكافحة جرائم تقنية المعلومات الإماراتي..

لقد شهدت العديد من الدول الأوروبية والعالمية اهتمامًا كبيرًا بتنظيم مجال تقنية المعلومات ومكافحة جرائمها. وقد اتخذت العديد من الجهود التشريعية لمكافحة ظاهرة الإجرام المعلوماتي.ومن بين هذه الجهود، صدرت العديد من القوانين والتشريعات في الدول التالية(١):

١ – **موقف المشرع السويدي**: حيث أصدر المشرع السويد عام ١٩٧٣ أول قانون لها في مجال مكافحة تقنية المعلومات وهو قانون البيانات السويدي، الذي يهتم بمعالجة قضايا الدخول غير المشروع للبيانات الحاسوبية، أو تزويرها، أو تحويلها، أو الحصول غير المشروع عليها، وهي بذلك تعتبر أول دولة تصدر تشريعات تتعلق بجرائم التقنية، لاسيما التزوير المعلوماتي.

٢- **موقف المشرع الدنماركي**: قد لحقت الدنمارك السويد في هذا التطور الحاصل في مجال تقنية المعلومات بإصدارها أول قانون لها يتعلق بمكافحة جرائم الحاسب الآلي والإنترنت عام ١٩٨٥، وكان من أهم نصوص هذا القانون تحديد العقوبات والأفعال المجرمة التي تعد انتهاكًا للحاسب الآلي كالتزوير المعلوماتي.

٣- **موقف المشرع البريطاني**: إصدار المشرع البريطاني قانون مكافحة التزوير والتزييف عام ١٩٨٦، وعرف أداة التزوير بأنها عبارة عن وسائط التخزين الحاسوبية المتنوعة، أو أي أداة أخرى يتم التسجيل عليها، سواء بالطرق التقليدية

(١) د/ ربيع محمود الصغير، القصد الجنائي، دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٥،ص ٩٦ .

أو الإلكترونية أو بأي طريقة أخرى.

٤- **موقف المشرع الأمريكي**: المشرع في الولايات المتحدة الأمريكية قام بإصدار العديد من التشريعات المتعلقة بتقنية وتكنولوجيا المعلومات، منها قانون تشريعي عام رقم ١٠٠-٩٩-٤٧٤ الذي تضمن العديد من القوانين السابقة والمعدلة منها، مثل القانون التشريعي رقم ١٢١٣ لعام ١٩٨٦ والمعدل (١٠٣٠ s، u 18،s) الخاص بمكافحة جرائم الحاسوب.

كما تجمع المجلس الأوروبي في العاصمة المجرية بودابست عام ٢٠٠١ للتشاور حول جرائم تقنية المعلومات والاتفاق على بنود واضحة لمكافحتها. وتم توقيع الاتفاقية الأوروبية الدولية لمكافحة الإجرام السيبراني (الإجرام عبر الإنترنت) من قبل ٣٠ دولة، وأضيفت إليها دول أخرى من خارج المجلس الأوروبي، وكانت الولايات المتحدة الأمريكية من بين هذه الدول، وقد صادقت على الاتفاقية في ٢٢ سبتمبر ٢٠٠٦ ودخلت حيز النفاذ في ١ يناير ٢٠٠٧. وتشمل الاتفاقية العديد من جوانب جرائم الإنترنت، بما في ذلك الإرهاب وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.

ثالثًا- الجهود التشريعية العربية في مجال مكافحة جرائم تقنية المعلومات:

على الجانب التشريعي العربي فهناك العديد من الدول العربية التي واكبت هذا التطور التقني الحاصل في مجال تكنولوجيا المعلومات وعملت على محاولة التصدي لمكافحة الجرائم الالكترونية الناشئة عنه بإصدارها عدد من التشريعات الخاصة، ومن بين هذه الدول ما يلي:

١ – **موقف المشرع المصري**: أصدر المشرع المصري العديد من التشريعات

التي تهدف إلى مواكبة التطور التكنولوجي والمعلوماتي في العصر الحديث، وتأمين نقل وتبادل المعلومات عبر شبكة الإنترنت(١). ومن هذه التشريعات، قانون تنظيم الاتصالات رقم ١٠ لعام ٢٠٠٣ م، والقانون رقم ١٥ لعام ٢٠٠٤ م بشأن تنظيم التوقيع الإلكتروني، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات لتأمين معاملات الأفراد عبر شبكة الإنترنت(٢). كما أصدر الدستور المصري لعام ٢٠١٤ م العديد من المواد التي تهدف إلى إقرار حماية خاصة لمختلف نواحي التعاملات التقنية والرقمية وتنظيمها(٣). ولا تزال هناك العديد من الدراسات القانونية والجهود التشريعية التي تبذل من أجل تأمين المعاملات الإلكترونية المختلفة من كافة جوانبها القانونية والجنائية. كما أنشأت مصر مجلسًا أعلى للأمن السيبراني لمواجهة

(١) انظر: المادة الأولي من هذا القانون وسائل الاتصالات بأنها: أية وسيلة لإرسال أو استقبالالرموز، أو الإشارات، أو الرسائل، أو الكتابات أو الصور، أو الأصوات، وذلك أيـًا كانت طبيعتها، وسواء كان الاتصال سلكيـًا أو لاسلكي، وقد اقر المشرع في الباب السابع من هذا القانون مجموعة من العقوبات التي تطبق إزاء التعرض أو الاعتداد على تلك الخدمات أو استغلالها بطرق غير مشروعة.

(٢) انظر: القرار بقانون رقم ١٥لسنة ٢٠٠٤م بشأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩لسنة -٢٠٠٥ شأن إصدار اللائحة التنفيذية لقانون التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

(٣) انظر: المادة رقم ٣١من الدستور المصري لعام ٢٠١٤على أن " أمن الفضاء المعلوماتى جزءمن منظومة الاقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليها، على النحوالذي ينظمه القانون". كما تنص المادة ٥٧من ذات الدستور على أن " للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها منوسائل الاتصال حرمه، وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها، أو رقابتها إلا بأمرقضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك.

الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها، وذلك بموجب قرار مجلس الوزراء رقم ٢٢٥٩ لعام ٢٠١٤م. كما قامت مصر بالانضمام إلى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، وذلك بموجب القرار الصادر عن رئيس الجمهورية القرار رقم ٢٧٧ لعام ٢٠١٤ م بتاريخ ١٩ سبتمبر عام ٢٠١٤ م. وأخر هذه التطورات التشريعية هو القانون رقم ١٧٥لعام ٢٠١٨ م الصادر بشأن مكافحة جرائم تقنية المعلومات، ولائحته التنفيذية رقم ١٦٩٩لعام٢٠٢٠م ويهدف هذا القانون إلى مكافحة جرائم تقنية المعلومات وحماية البيانات الشخصية والحقوق الملكية الفكرية والأمن السيبراني، ويعد إضافة هامة للمساعي الرامية إلى تأمين المعاملات الإلكترونية في مصر(١).

٢- **موقف المشرع الإماراتي**: دولة الإمارات العربية المتحدة كان لها اهتمام واضح بمكافحة الجريمة المعلوماتية والتصدي لأخطارها، وقد أصدرت العديد من التشريعات المتعلقة بهذه النوعية من الجرائم المعلوماتية عالية التقنية. من بين هذه التشريعات القانون العربي الاسترشادي الصادر عام ٢٠٠٣ بشأن مكافحة جرائم تقنية المعلومات وما في حكمها، والقانون الخاص بمكافحة جرائم تقنية المعلومات الصادر عام ٢٠٠٦م، والقانون الخاص بإنشاء الهيئة الوطنية للأمن الالكتروني

(١) إنظر: قرار وزير الاتصالات ١٠٧لسنة٢٠٠٥بشأن مكتب حماية برامج الحاسب الآلي وقواعد البيانات.، قرار وزير الاتصالات ١٢٨لسنة٢٠٠٦بشأن اختصاص الجهاز القومي لتنظيم الاتصالات بنظر المنازعات المتصلة بالاتصالات، وإنشاء إدارة تسمى إدارة فض المنازعات بالجهاز، قرار وزير الاتصالات رقم ١٠٨لسنة ٢٠٠٥ بشأن تحديد الخدمات والأعمال الخاضعة لرسم تنمية صناعة تكنولوجيا المعلومات والاتصالات .

الصادر عام ٢٠١٢م. وتعتبر دولة الإمارات العربية المتحدة أول دولة عربية تقوم بإصدار تشريع قانوني مستقل يتعلق بمكافحة الجرائم المعلوماتية، وهو القانون رقم ٢ لعام ٢٠٠٦م. وتم تعديل هذا القانون في عام ٢٠١٨ م بواسطة المرسوم الاتحادي رقم ٢ لعام ٢٠١٨م.

٣ - موقف المشرع السعودي: أصدر المشرع السعودي عام ٢٠٠٧ م نظام مكافحة الجرائم المعلوماتية الذي يحدد الجرائم المعلوماتية والعقوبات المقررة لكل منها، ويهدف إلى الحد من وقوع جرائم المعلوماتية وحماية الأمن المعلوماتي وحماية المصلحة العامة والاقتصاد الوطني. وتم التصديق على هذا النظام بالمرسوم الملكي رقم ١٧ م بتاريخ ٨/ ٣/ ١٤٢٨هـ، وصدر بالقرار الوزاري رقم ١١٥٦٧ بتاريخ ٩/ ٣/ ١٤٢٨هـ.

المطلب الثاني : تطور قواعد الاختصاص والقانون الواجب التطبيق

تثير الجرائم المعلوماتية العديد من المشكلات نظراً لطبيعتها الخاصة المعقدة والسرعة التي يتم فيها ارتكابها، وقدرة الجناة على الهرب والتخفي. بالإضافة إلى أنها جرائم عابرة للحدود والقارات، فقد يتم ارتكاب هذه الجرائم داخل نطاق إقليمي لدولة وتحقيق آثارها خارج هذا النطاق، مما يؤدي إلى تعقيدات كبيرة في تحديد الاختصاص القانوني والقضائي لهذه الجرائم الجديدة، وضرورة التعاون الدولي في مجال مكافحتها(١). كما تترتب على انتشار العولمة وسهولة تداول المعلومات عبر الحدود واتصال الكمبيوتر بشبكات دولية ظهور فئة جديدة من

(١)د/ مروي السيد الحصاوي، مبدأ العالمية في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠١٩،ص١٠٠ .

الجرائم التي تعتمد بشكل كبير على التقنيات الحديثة. وتختلف هذه الجرائم في طريقة انتشارها وتأثيرها عن الجرائم التقليدية، حيث تنتشر بشكل أسرع وتؤثر بشكل أكبر على عدة دوائر. وتؤثر هذه الجرائم أيضًا على سلطة الدولة في مجال التجريم والعقاب، نظرًا لطبيعتها العابرة للحدود الدولية(١). وقد أدت عولمة الشبكة الإلكترونية إلى ظهور جرائم دولية، حيث يمكن وقوع هذه الجرائم في أكثر من دولة في نفس الوقت أو وقوع أجزاء من نفس الجريمة في دول مختلفة. وهذا يستدعي الجدل حول القانون الذي يجب تطبيقه على هذه الجرائم؛ فهل يجب تطبيق قانون الدولة التي وقع فيها النشاط الإجرامي أم قانون الدولة التي حدثت فيها النتيجة؟(٢) وماذا يحدث إذا كان قانون إحدى الدول لا يعترف بتلك الجريمة أو يعتبرها غير قانونية؟ يجب بالتأكيد إعادة النظر في هذه المسائل ووضع قوانين دولية مناسبة لمكافحة هذه الجرائم الجديدة. وتزايدت التحديات المتعلقة بالجرائم الإلكترونية والعابرة للحدود الدولية في العقدين الماضيين، مما دفع بالفقه الجنائي والدولي إلى إعادة النظر في مفهوم السيادة المطلقة للدولة(٣) على إقليمها واعتماد فكرة السيادة

(١) د/ كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، بحث منشور ضمن أعمال المؤتمر العلمي السادس للجمعية المصرية للقانون الجنائي، ،١٩٩٣، ص٣٢ .

(٢) د/ محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)،أعمال المؤتمر السادس الجمعية المصرية للقانون الجنائي، دار النهضة العربية،١٩٩٣، ص٣٥.

(٣) د/ عمر الفاروق الحسيني ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، أعمال المؤتمر السادس الجمعية المصرية للقانون الجنائي، دار النهضة العربية ، ، ١٩٩٣، ص ٤٥ .

النسبية. قد يؤدي ذلك في المستقبل إلى فكرة انعدام السيادة على الجرائم العابرة للحدود،(١) والتنازل عنها لصالح فكرة "عالمية القانون الجنائي"، والتي تحكم قضايا القوانين الواجبة التطبيق والمحاكم صاحبة الولاية في مثل هذه الجرائم.

وعلى المستوى الدولي، بدأت قوانين الإجراءات الجنائية والقوانين ذات الصلة بالجرائم المتعلقة بالمعلوماتية في التحول تدريجيًا من المبادئ التقليدية، مثل مبدأ الاختصاص الوطني لمحاكم الدولة والقوانين الواجبة التطبيق، إلى مبادئ جديدة مثل مبدأ العالمية. وتم عقد اتفاقيات دولية لترتيب هذه المسائل بما يحقق ضمان الملاحقة وعدم الإفلات من العقاب(٢).

أولاً- النطاق المكاني للقانون وتحديد الاختصاص القضائي:

يتم تطبيق قانون العقوبات في إقليم الدولة على جميع الجرائم المرتكبة فيه، سواء كان الجاني وطنيًا أو أجنبيًا، وسواء كان المجني عليه وطنيًا أو أجنبيًا. يتم الاعتماد على مبدأ الإقليمية في تطبيق هذا القانون، ويرجع ذلك إلى أن قانون العقوبات يعبر عن سيادة الدولة. وعندما يتم ارتكاب جريمة في إقليم الدولة، يصبح تطبيق قانون العقوبات واجبًا، ويتم محاكمة المتهمين بالجريمة بغض النظر عن

(١) د/ جلال ثروت، نظم القسم العام في قانون العقوبات المصري، منشأة المعارف، الاسكندرية، ١٩٨٩،ص١٠.

(٢) د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة ، أسيوط، ١٩٩٤ ، ص ٥.

جنسيتهم أو ديانتهم. ومع ذلك، فإن قانون مكافحة جرائم تقنية المعلومات يتبنى مبدأ العينية طبقا لمبدأ الإقليمية المتبع في قانون العقوبات العام. ويتم تطبيق أحكام هذا القانون على جميع الجرائم المرتكبة خارج إقليم مصر، وحتى لو ارتكبها أجانب، شريطة أن يكونوا معاقبين على نفس الفعل في الدول التي ارتكبوا فيها الجريمة، طبقا لمبدأ الإقليمية(١). وتم تطبيق مبدأ العينية على قانون العقوبات في مصر، حيث يتم محاسبة الجرائم التي ترتكب في خارج البلاد وتتعلق بمصالح جوهرية للدولة، بغض النظر عن جنسية الفاعل في تلك الجرائم. ولقد تم تطبيق مبدأ العالمية الجنائية على الجرائم التي تتعلق بتقنية المعلومات وتحدث خارج البلاد، وذلك طبقا لمبدأ الإقليمية السلبية الذي يسمح للدولة بالمتابعة الجنائية ضد المرتكبين على أساس جنسية المجني عليهم(٢). ومن أهم الأمور التي نظمها المشرع المصري في قانون مكافحة جرائم تقنية المعلومات، هي النطاق المكاني لتطبيق القانون، حيث تم تحديد النطاق المكاني لتطبيق القانون بمبدأ العينية بدلاً من المبدأ الإقليمي. وتم إسناد مهمة الاختصاص القضائي للقاضي الوطني، حتى وإن لم يرد النص على هذا الاختصاص صراحة، وذلك تحت المادة الثالثة من قانون

(١) د/ سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠، ص١٢٥ .

(٢) د/ أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ١٩٩٩، ص١١٦ .

مكافحة جرائم تقنية المعلومات. تتضمن المادة الثالثة من هذا القانون تحديد حالات تطبيق القانون من حيث المكان على الجرائم المعلوماتية التي ترتكب خارج حدود الدولة المصرية. وبموجب هذه المادة، يتم تطبيق أحكام القانون على الأشخاص الذين يرتكبون جرائم في الخارج من غير المصريين، إذا كان الفعل معاقبًا عليه في الدولة التي وقع فيها الفعل، تحت أي وصف قانوني. على النحو التالي:

١ – إذا ارتكبت الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها .

٢ – إذا كان المجني عليهم أو أحدهم مصريـًا .

٣ – إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها في مصر .

٤ – إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها مصر .

٥ – إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأي من مصالحها، في الداخل أو الخارج .

٦ – إذا وجد مرتكب الجريمة في مصر، بعد ارتكابها ولم يتم تسليمه.

يمكن القول إن المشرع المصري قد تميز في تبنيه للاتجاه المتمثل في تحديد النطاق المكاني لتطبيق أحكام القانون وتحديد حدود سريانه بشكل واضح، سواء فيما

يتعلق بالجناة أو المجني عليهم، وكذلك في تحديد القاضي الجنائي المختص بنظر هذه الجرائم، وهذا يتفق مع ما ورد في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

وفي المادة ٣٠ من الفصل الرابع من الاتفاقية العربية، جرى تحديد القاضي المختص بنظر هذه الجرائم، حيث نصت الاتفاقية على أن يكون لقاضي الدولة التي وقعت الجريمة صلاحية النظر في الجرائم التي ارتكبت داخل حدود دولته، أو التي كان لها تأثير عليها، أو التي ارتكبت من خلال أجهزة الاتصالات أو الشبكات الإلكترونية التي تخضع للرقابة أو الرخصة في دولته.

وبناء على ذلك، يمكن القول إن المشرع المصري قد حسن صياغة النص في هذا الجانب، حيث جعل من السهل تحديد النطاق المكاني لتطبيق أحكام القانون، وكذلك تحديد القاضي المختص بنظر الجرائم التي تتعلق بتقنية المعلومات.

١ – تتعهد كل دولة طرف باتخاذ الإجراءات اللازمة لتوسيع اختصاصها لتشمل أيًا من الجرائم المشار إليها في الفصل الثاني من هذه الاتفاقية، سواء ارتكبت الجريمة كليًا أو جزئيًا، أو تم تحقيقها بأي شكل من الأشكال.

- في إقليم الدولة الطرف.
- على متن سفينة تحمل علم الدولة الطرف.
- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.
- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

٢ - يتعين على كل دولة طرف اتخاذ الإجراءات اللازمة لتوسيع الاختصاص الذي يغطي الجرائم المشار إليها في المادة ٣١ فقرة (١) من هذه الاتفاقية، في الحالات التي يتواجد فيها المشتبه به في إقليم تلك الدولة الطرف ولا يتم تسليمه إلى طرف آخر بناءً على جنسيته بعد طلب التسليم.

كما ينص القانون الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات على أن القانون ينطبق على جميع الأفعال الجنائية التي ترتكب باستخدام تقنية المعلومات في دولة الإمارات العربية المتحدة، سواء كانت هذه الأفعال تؤثر على أمن الدولة أو الأفراد أو المؤسسات أو الممتلكات أو السلامة العامة. ويتم تحديد الاختصاص القضائي في قضايا جرائم تقنية المعلومات وفقًا لأحكام القانون الإماراتي للإجراءات الجنائية والقوانين ذات الصلة، ويمكن للمحاكم الإماراتية تقدير الاختصاص القضائي على أساس موقع الجريمة والجناية المرتكبة، ومكان إقامة المتهم أو المتضرر، ومكان تخزين البيانات أو حدوث الاختراق أو الاعتداء السيبراني، وغيرها من العوامل ذات الصلة.

ويمكن للجهات القضائية في الإمارات تطبيق القانون الإماراتي على الجرائم التي

ترتكب خارج الإمارات وتؤثر على الأمن القومي أو تستهدف المواطنين أو المقيمين في الإمارات أو تتعلق بممتلكات أو مصالح في الإمارات. (١).

ثانيًا: مجال التنازع القضائي المحلي :

تنص المادة الرابعة من القانون رقم ١٢٠ لعام ٢٠٠٨م ، الذي ينص على إنشاء المحاكم الاقتصادية وتعديلاته، على أن مهمة الفصل في النزاعات وجرائم الجنح التي تنشأ نتيجة تطبيق أحكام هذا القانون تسند إلى المحكمة الاقتصادية بدوائرها المختلفة. وتختص الدوائر الابتدائية والاستئنافية بالمحاكم الاقتصادية، وحدها، بنظر الدعاوى الجنائية الناشئة عن الجرائم المنصوص عليها في القوانين التالية:

- قانون حماية حقوق الملكية الفكرية.
- قانون تنظيم الاتصالات.
- قانون تنظيم التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا

(١) انظر: المادة ٢٦ من القانون الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات:
"يجوز للمتضرر من جريمة تقنية معلوماتية، أو وكيله القانوني، أو وكيل المصلحة العامة، أو الجهات المختصة، أو أي شخص حائز على صك أو تفويض من المتضرر، أن يتقدم بشكوى إلى الجهات الأمنية والقضائية المختصة في الدولة، ويجب على الجهات الأمنية والقضائية المختصة التعامل مع هذه الشكاوى وفقًا لأحكام القوانين والأنظمة المعمول بها في الدولة، ويجوز لها اتخاذ الإجراءات اللازمة لحفظ الأدلة والتحقق من صحة الشكاوى، وتطبيق العقوبات المنصوص عليها في هذا القانون على المتهمين في حالة إدانتهم بارتكاب جرائم تقنية المعلومات."

المعلومات.

ونظرًا لتشابه جرائم التقنية المعلوماتية الواردة في القانون رقم ١٧٥ لعام ٢٠١٨ م إلى حد كبير مع تلك المشار إليها في المادة الرابعة المذكورة أعلاه، فإن ذلك يؤكد تفرد واستقلال المحكمة الاقتصادية بدوائرها المختلفة فيما يتعلق بمكافحة جرائم تقنية المعلومات، وبالتالي فإنها ليست بحاجة إلى إضافة نص صريح على ذلك(١). كما ينص القانون الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات على أن التنازع القضائي المحلي يتم تحديده وفقًا لأحكام القانون الإماراتي للإجراءات الجنائية والقوانين ذات الصلة. وينص القانون أيضًا على أنه يمكن للمتضررين من جرائم تقنية المعلومات التقدم بشكوى إلى الجهات الأمنية والقضائية المختصة في دولة الإمارات العربية المتحدة، ويتم التعامل مع هذه الشكاوى وفقًا لأحكام القوانين والأنظمة المعمول بها في الدولة. ويتم التحقق من صحة الشكاوى وجمع الأدلة اللازمة وإجراء التحقيقات اللازمة للوصول إلى الحقيقة، ويمكن للمدعي العام أو المحكمة المختصة في الإمارات العربية المتحدة أن تصدر أمراً بالاستدعاء للمتهمين وإجراء التحقيقات اللازمة، ويتم تطبيق العقوبات المنصوص عليها في القانون الإماراتي على المتهمين في حالة إدانتهم بارتكاب جرائم تقنية المعلومات. ويجب على جميع الأطراف المشاركة في التنازع القضائي المحلي أن يتبعوا الإجراءات المقررة في القانون الإماراتي والأنظمة ذات

(١) انظر: الطعن رقم ٧٨٤٣لسنة ٨٧ق، مجموعة أحكام محكمة النقض المصرية ، جلسة ٢٠ / ١/ ٢٠١٩ .

الصلة، ويتم تطبيق القوانين المعمول بها في الدولة على جميع الأفراد والجهات المتورطة في جرائم تقنية المعلومات(١).

ثالثًا: مجال التنازع القضائي الدولي :

تولي الاتفاقية العربية اهتمامًا ملحوظًا بمسألة تحديد القاضي الجنائي المختص بنظر الجرائم المعلوماتية التي ترتكب بواسطة وسائل التقنية الحديثة، وتعمل على وضع الحلول للنزاعات التي قد تنشأ بشأن التنازع القضائي، سواء كان هذا التنازع تنازعًا إيجابيًا بادعاء أكثر من دولة باختصاصها القضائي بنظر جريمة تقنية، أو تنازعًا سلبيًا وهو تخلي وإنكار للدول عن اختصاصها القضائي. وقد وضعت الاتفاقية شروطًا لتحديد القاضي المختص بنظر هذه الجرائم، وذلك وفقًا لدرجة الخطورة أو الضرر الواقع على الدولة ودرجة المساهمة الإجرامية، وضرورة أن تكون الدولة طرفًا في الاتفاقية العربية المبرمة(٢).

وأولى الاتفاقية أهمية كبيرة لقاضي الدولة التي أخلت الجريمة بأمنها ومصالحها وتسببت في الإضرار بها، وجعلته في مقدمة القضاة المختصين ليكون هو صاحب الاختصاص الأصيل والأولي في تبني إجراءات المحاكمة والعقاب. وعلى الرغم من أهمية هذه الإشكالية المتمثلة في تنازع الاختصاص القضائي، إلا أنه لم يتم الإشارة إليها بصراحة ضمن أحكام ونصوص قانون جرائم التقنية المعلوماتية في

(١) انظر: المادة ٢٧ من القانون الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات.

(٢) انظر: الفقرة الثالثة من المادة ٣٠من الاتفاقية العربية لمكافحة الجريمة المعلوماتية.

المشرع المصري، ولذلك يجب إجراء تعديل لنصوص هذا القانون لتحديد القاضي المختص بنظر هذه الجرائم بصراحة، والتبني للاتجاه الوارد بالاتفاقية العربية لمكافحة جرائم التقنية. ويتمثل تحديد القاضي المختص بنظر هذه الجرائم وفقًا للاتفاقية العربية في أن يكون لقاضي الدولة التي وقعت الجريمة على إقليمها الأولوية في الاختصاص، حتى وإن لم ينتج عنها ضرر أو تهديد أمني لهذه الدولة، ثم يكون الاختصاص لقاضي الدولة التي ينتمي إليها الجاني أو الجناة، أي لقاضي الدولة التي يكون الشخص المطلوب من رعاياها، ويتم تحديد الاختصاص لقاضي الدولة الأسبق في تقديم طلب التسليم للمحاكمة في حالة اتحاد الظروف المشار إليها. كما أن مجال التنازع القضائي الدولي في مكافحة جرائم تقنية المعلومات الإماراتي يشمل كافة الجرائم التي تتعلق بالتكنولوجيا والمعلومات، مثل جرائم الاحتيال الإلكتروني، والاختراق الإلكتروني، والتجسس الإلكتروني، والتهديد الإلكتروني، والتحريض على الجرائم الإلكترونية، والقرصنة الإلكترونية، وجرائم الإبلاغ الزائف، والتعرض للمعلومات السرية والخاصة، وجرائم الإنترنت والاتصالات، والجرائم التي تتعلق بالإنترنت المظلم، وغيرها من الجرائم الإلكترونية.

ويتم التعامل مع هذه الجرائم في الإمارات العربية المتحدة وفقًا للقوانين والتشريعات المحلية، وتتولى الجهات المختصة في الدولة مثل الشرطة والنيابة العامة والمحاكم والهيئات القضائية مكافحة هذه الجرائم ومعالجتها قانونيًا.

وفي حالة وجود تنازع قضائي دولي فيما يتعلق بهذه الجرائم، يتم التعامل معه

وفقًا للاتفاقيات الدولية والإقليمية المتعلقة بمكافحة الجرائم الإلكترونية، والتي تشمل تبادل المعلومات والأدلة بين الدول والتعاون في مجال التحقيق والملاحقة الجنائية، وذلك من خلال القنوات الرسمية المتاحة بين الدول(١).

تعقيب:

رغم أهمية إشكالية تنازع الاختصاص القضائي في جرائم التقنية المعلوماتية، إلا أنه لم يتم تناولها بصراحة ضمن نصوص قانون جرائم التقنية المعلوماتية في مصر. وبالتالي، ينبغي على المشرع المصري إجراء تعديلات على هذا القانون لضمان تنظيم وتحديد القاضي المختص بنظر هذه الجرائم بشكل صريح، وتبني الاتجاه المتضمن في الاتفاقية العربية لمكافحة جرائم التقنية المعلوماتية. ونوصي بأن يولي المشرع المصري هذه الإشكالية الكبيرة الاهتمام اللازم لحماية الأمن الإلكتروني والعدالة القضائية.

المطلب الثالث

(١) انظر: الاتفاقيات الدولية التي تتعلق بمكافحة الجرائم الإلكترونية والتي تشمل التعامل مع التنازع القضائي الدولي، يمكن ذكر اتفاقية مجلس أوروبا لمكافحة جرائم الإنترنت، والتي وافقت عليها الإمارات العربية المتحدة في عام ٢٠١٣. وتنص المادة ٢٥ من هذه الاتفاقية على ضرورة التعاون الدولي وتوفير المساعدة الممكنة بين الدول في مجال مكافحة جرائم الإنترنت، وتشمل هذه المساعدة تبادل المعلومات والأدلة والخبرات والتعاون في مجال التحقيق والملاحقة الجنائية. وتنص المادة ٢٦ على ضرورة توفير الحماية الملائمة للأدلة والمعلومات والتي تكون ضرورية في التحقيق والملاحقة الجنائية، وتشمل هذه الحماية الإجراءات اللازمة للحفاظ على سرية المعلومات والأدلة وعدم الكشف عنها إلا بموجب ترخيص قانوني.

حجية الدليل الرقمي
في الإثبات الجنائي للجرائم المعلوماتية

يشير التطور التكنولوجي إلى ظهور وسائل جديدة للإثبات الجنائي، وهذا أدى إلى الاعتراف بالحجية القانونية للأدلة المستمدة من الوسائل العلمية في مرحلة التحقيق ومرحلة المحاكمة. وقد أدى هذا التطور إلى تبني بعض التشريعات الجنائية لمبدأ رقمنة الإجراءات الجنائية، مثل التشريع الفرنسي والإماراتي والمغربي. ودعا بعض الفقه المصري إلى استحسان هذا النظام والدعوة للأخذ به في القانون المصري(١). وفيما يلي، سنعرض على هذين الجزئيتين بشيء من التفصيل.

أولاً: الاعتراف بالأدلة الرقمية وحجيتها في الإثبات :

تختلف آراء الفقهاء في بعض المسائل المتعلقة بالإثبات الجنائي، مثل مسألة تفتيش الحواسيب الآلية والبريد الإلكتروني وقابلية الشبكات الإلكترونية للمراقبة والتفتيش، وما هي القيمة القانونية للأدلة المستخلصة منها. ومع ذلك، توصلت الأراء إلى أنه يمكن اتخاذ هذه الإجراءات حيال الكيانات المنطقية وغير الملموسة، وأن الأدلة الرقمية يمكن الاعتراف بها بالحجية القانونية في الإثبات بما يوازي الأدلة المادية العادية المستنبطة من الإجراءات التقليدية. ويشير هذا التطور في فلسفة الاثبات في الدعوى الجنائية إلى تطور كبير في السياسة الجنائية، حيث يتم الاعتراف

(١) د/ أشرف عبد الستار، رقمنة الإجراءات الجنائية في ظل جائحة كورونا، بحث مقدم للمؤتمر السنوي الحادي والعشرون مركز البحوث الاجتماعية والجنائية، القاهرة ٢٧ حتى 29/ 9 / 2021 ، ص٧.

بالأدلة الرقمية الجديدة وتطبيقها في القانون(١). كما تشمل الأدلة الرقمية كل البيانات أو المعلومات التي يمكن إعدادها أو تخزينها في شكل رقمي، وتجد أساسها في البيئة الرقمية الافتراضية، ويمكن استخدامها للإشارة إلى ارتكاب جريمة جنائية. وعلى أثر ذلك، بدأ الاعتراف بالمحررات الإلكترونية والتوقيع الإلكتروني في تشريعات العديد من الدول. كما تشمل أيضا الأدلة الرقمية الصور الرقمية التي تجسد الحقائق المرئية حول الجريمة، وتعتبر بديلاً تكنولوجيـًا للصور الفوتوغرافية التقليدية، حيث يمكن استخدامها في الإثبات والدفاع عن النفس. كما تتضمن الأدلة الرقمية التسجيلات الصوتية، وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الأليات الرقمية، وتشمل المحادثات الصوتية. ويمكن أيضًا أن تتضمن الأدلة الرقمية النصوص المكتوبة، والتي تم إنشاؤها باستخدام الأدوات الإلكترونية، مثل رسائل البريد الإلكتروني، والرسائل النصية، والبيانات المخزنة في الحاسوب وغيرها. ويمكن استخدام هذه الأدلة للإشارة إلى وجود جريمة أو نفيها، وتستخدم في الإثبات الجنائي والدفاع عن النفس. كما تنص المادة الأولى من قانون مكافحة جرائم تقنية المعلومات الدليل الرقمي على أن الأدلة الإلكترونية المأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية والتي يمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة، تعد معلومات إلكترونية لها قوة

(١) د/ عمر محمد أبو بكر يونس، الإ جراءات الجنائية عبر الإنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش نظم الحاسب الآلي وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، دار الفكر العربي، القاهرة، ٢٠٠٥، ص ٢١.

أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة، وتشمل ما في حكمها(١).

وفي المادة الحادية عشر من القانون، يقر المشرع المصري بقيمة الأدلة الرقمية المستمدة من وسائل التقنية الحديثة(٢)، ويمنحها القيمة القانونية والحجية الثبوتية الممنوحة للأدلة الجنائية المادية في الإثبات الجنائي(٣)، المقررة بموجب قانون الإجراءات الجنائية المصري رقم ١٥٠لسنة ١٩٥٠ وتعديلاته، وقواعد الإثبات المتعارف عليها فقهـاً وقضاءً وقانونـاً(٤).

وتشترط المادة الأولى من القانون الحصول على شروط ومواصفات معينة لقبول الأدلة الرقمية في الإثبات، والتي تختلف عن الأدلة المادية التقليدية(٥)، ويحيل المشرع المصري في الفقرة الأخيرة من المادة المذكورة إلى النصوص الواردة في اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات، والتي تحدد

(١) انظر : المادة الأولي من قانون تقنية المعلومات المصري الصادر في شأن مكافحة جرائم التقنية.

(٢) د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، الطبعة الثالثة ، ١٩٩٨م، ص٧٦٦.

(٣) د/ على محمود على، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي، مركز البحوث والدراسات ، عام ٢٠٠٣، ص٢٨١.

(٤) د/ عائشة مصطفي، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ، دراسة مقارنة ، رسالة ماجستير، كلية الحقوق، جامعة الإسكندارية ، ٢٠٠٩، ص١٨.

(٥) د/ طارق فوزي ، الجوانب الإجرائية في الجرائم المعلوماتية ، رسالة دكتوراة، كلية الحقوق ، جامعة المنوفية، ٢٠١١، ص١٩٥.

الشروط والضوابط والمواصفات الفنية المعينة التي تمنح الأدلة الرقمية هذه القوة الثبوتية(١). وتنص اللائحة التنفيذية للقانون، الصادرة بموجب قرار مجلس الوزراء رقم ١٦٩٩ لعام ٢٠٢٠م، على شروط وضوابط يجب توافرها في الدليل التقني لقبوله والاعتراف بحجيته وقيمته الثبوتية، إضافة إلى الإجراءات المعينة واللازمة لتقديم هذا الدليل أمام الجهات المختصة. ويتعين على الدليل التقني توافر شروط منها، عدم التعديل في البيانات والمعلومات الإلكترونية، وضمان عدم التلاعب بها بأي شكل من الأشكال، وضمان استخدام تقنيات تضمن سلامة البيانات وثباتها، وتحديد مصدر البيانات وتوثيقه، وتوفير سجلات تفصيلية للعمليات المنجزة على البيانات والمعلومات.

ويتضمن الدليل التقني أيضـًا إجراءات لتقديمه أمام الجهات المختصة، ومن ضمنها تقديم طلب رسمي للجهة المعنية، وتوثيق الدليل والإجراءات المتبعة في إعداده، وتزويد الجهة المختصة بنسخة من الدليل، بالإضافة إلى إجراءات أخرى تختلف باختلاف الجهة المختصة ونوع الدليل المقدم. كما قام المشرع الإماراتي بإصدار قانون الجرائم المعلوماتية رقم ٥ لعام ٢٠١٢م، والذي يتضمن أحكامـًا

(١) انظر: المادة الحادية عشر من ذات القانون على أن " يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتى أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

تتعلق بالإثبات الجنائي في جرائم المعلوماتية. ويتطلب القانون الإماراتي الدليل الرقمي كوسيلة لإثبات الجرائم المعلوماتية، ويشمل هذا الدليل الرقمي العديد من العناصر، مثل سجلات الخوادم والمعلومات الإلكترونية والبيانات الرقمية الأخرى. ويعتبر الدليل الرقمي مقبولًا كدليل في المحاكم الإماراتية، بشرط أن يتم تأكيده وفقًا للإجراءات القانونية المنصوص عليها في القانون الإماراتي. ويتم تأكيد الدليل الرقمي عن طريق مركز الأدلة الجنائية والعلمية التابع لشرطة دبي، حيث يتم تحريز الأجهزة والأدلة الرقمية وتحليلها وتأكيدها بما يتماشى مع الإجراءات القانونية. ويمكن للمتهمين في جرائم المعلوماتية في الإمارات الدفاع عن أنفسهم باستخدام الدليل الرقمي أيضًا، حيث يمكنهم توفير الأدلة الرقمية التي تدعم دفاعهم. ويمكن للمحاكم الإماراتية أن تستخدم هذه الأدلة الرقمية كدليل في القضايا المتعلقة بجرائم المعلوماتية، شريطة تأكيدها وفقًا للإجراءات القانونية المنصوص عليها في القانون الإماراتي(١).

ثانيـًا : الشروط والمواصفات الواجب توافرها في الدليل التقني: فقد حددت المادة التاسعة من القانون رقم ١٧٥ لعام ٢٠١٨م ولائحته التنفيذية بشأن مكافحة جرائم تقنية المعلومات المصري الشروط والضوابط والمواصفات بنصها على أن تحوز الأدلة الرقمية ذات القيمة والحجية للأدلة الجنائية المادية في الإثبات

(١) انظر: المادة الثالثة من القانون رقم ٥ لعام ٢٠١٢م بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

الجنائي(١). إذ ينص القانون على أنه يجب توافر شروط معينة لجمع أو الحصول أو استخراج أو استنباط الأدلة الرقمية، وذلك باستخدام تقنيات على النحو التالي:

- عدم تغيير أو تحديث أو محو أو تحريف الكتابة أو البيانات والمعلومات، أو أي تغيير أو تحديث أو إتلاف للأجهزة أو المعدات أو البيانات والمعلومات، أو أنظمة للمعلومات أو البرامج أو الدعامات الإلكترونية وغيرها. ويشمل ذلك استخدام تقنيات مثل Write Blocker وDigital Images Hash وغيرها من التقنيات المماثلة التي تحافظ على سلامة وثبات البيانات والمعلومات المستخرجة أو المأخوذة، بحيث لا يتم تغييرها أو تحديثها أو محوها أو تحريفها أو إتلافها(٢).
- أن تكون الأدلة الرقمية ذات صلة بالواقعة وفي إطار الموضوع المطلوب إثباته أو نفيه، وفقًا لنطاق قرار جهة التحقيق أو المحكمة المختصة(٣).

---

(١) د/ أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، دراسة تحليلية مقارنة ، بحث منشور بمجلة البحوث القانونية والاقتصادية ، العدد ٧٦، ٢٠٢١م، ص٨٦.

(٢) د/ أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، دراسة تحليلية مقارنة ، بحث منشور بمجلة البحوث القانونية والاقتصادية ، العدد ٧٦، ٢٠٢١م، ص١٠٨.

(٣) د/ هلالى عبد الله أحمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٩٧، ص٢٥.

- أن يتم جمع الدليل الرقمي واستخراجه وحفظه وتحريزه بمعرفة مأموري الضبط القضائي المخول لهم التعامل في هذه النوعية من الأدلة، أو الخبراء أو المتخصصين المنتدبين من جهات التحقيق أو المحاكمة، وعلى أن يبين في محاضر الضبط، أو التقارير الفنية على نوع ومواصفات البرامج والأدوات والأجهزة والمعدات التي تم استخدامها، مع توثيق كود وخوارزمHash الناتج عن استخراج نسخ مماثلة ومطابقة للأصل من الدليل الرقمي بمحضر الضبط أو تقرير الفحص الفني، مع ضمان استمرار الحفاظ على الأصل دون عبث به (١).
- في حالة تعذر فحص نسخة الدليل الرقمي وعدم إمكانية التحفظ على الأجهزة محل الفحص لأي سبب يتم فحص الأصل ويثبت ذلك كله في محضر الضبط أو تقرير الفحص أو التحليل.
- أن يتم توثيق الأدلة الرقمية بمحضر إجراءات من قبل المختص قبل عمليات الفحص والتحليل له وكذا توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته(٢).

كما تشترط المادة الثانية من قانون التوقيع الإلكتروني الإماراتي رقم ١ لعام

(١) د/ حسين محمود ، الوسائل العلمية الحديثة في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٨١، ص٢٥.

(٢) د/ خالد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان ، ٢٠٠٠، ص٦٣٤.

٢٠٠٦ الشروط والمواصفات التالية للدليل التقني الإماراتي(١):

١- يجب أن يضمن الدليل التقني الإماراتي فعالية التوقيع الإلكتروني وسريته وصحته وأصالته.

٢- يجب أن يحتوي الدليل التقني الإماراتي على الإجراءات والمعايير والتقنيات اللازمة للتحقق من صحة التوقيع الإلكتروني ومصداقيته.

٣- يجب أن يكون الدليل التقني الإماراتي متوافقًا مع المعايير الدولية المتعلقة بالتوقيع الإلكتروني والأمان الإلكتروني.

٤- يجب أن يتم اعتماد الدليل التقني الإماراتي من قبل الهيئة الوطنية للمواصفات والمقاييس بعد دراسته وفحصه.

٥- يجب أن يتم تحديث الدليل التقني الإماراتي بشكل دوري ليتوافق مع التطورات التقنية والأمنية.

وتتمثل أهمية الشروط والمواصفات المذكورة في الحفاظ على سلامة التوقيع الإلكتروني وضمان صحته ومصداقيته، وهي تعكس التزام الإمارات بتعزيز الأمن الإلكتروني ودعم استخدام التوقيع الإلكتروني في العمليات التجارية والحكومية.

ثالثًا: إجراءات تقديم الدليل التقني من توثيق وتوصيف واعتماد: كما حددت المادة العاشرة من القانون رقم ١٧٥ لعام ٢٠١٨م ولائحته التنفيذية بشأن مكافحة

(١) انظر: المادة الثانية من القانون رقم ١ لعام ٢٠٠٦ بشأن الشروط والمواصفات للدليل التقني الإماراتي.

جرائم تقنية المعلومات المصري بشأن الإجراءات التي تنص على أن " يتم توصيف وتوثيق الدليل الرقمي من خلال طباعة نسخ من الملفات المخزن عليها أو تصويرها بأي وسيلة مرئية أو رقمية، واعتمادها من الأشخاص القائمين على جمع أو استخراج أو الحصول أو التحليل للأدلة الرقمية، مع تدوين البيانات. كما أقر المشرع صراحة بقيمة وحجية الأدلة الرقمية المستخرجة من الوسائل والأنظمة المعلوماتية التقنية، وأعترف بقوتها التدليلية في مجال الإثبات الجنائي. وبذلك، يكون المشرع قد أحسن صنعـًا من غيره في مواكبة التطورات الحاصلة في مجال تكنولوجيا المعلومات ووسائل التقنية الحديثة، وإدخالها في الأنظمة التشريعية والقضائية. ولا يختلف ذلك عن ما تم اعتماده في التشريعات الأوروبية والأجنبية في هذا الشأن، ومنها التشريع الإنجليزي الصادر عام ١٩٨٤ والمعمول به اعتباراً من عام ١٩٨٦، والذي يتعلق بالإثبات ويحوي تنظيمـًا محدداً لمسألة قبول مخرجات الإنترنت والحاسب الآلي كأدلة إثبات في المواد الجنائية، وكذلك قانون إساءة استخدام الحاسوب الذي صدر عام ١٩٩٠م. ويشمل التشريع الأمريكي المتعلق بالإثبات وقبول الأدلة والمخرجات الإلكترونية في عملية الإثبات، والاعتراف بقيمتها وقوتها التدليلية(١). وبذلك، يتماشى المشرع العربي مع التطورات الحديثة في مجال التكنولوجيا الحديثة، ويستخدم الأدلة الرقمية المستخرجة من الوسائل

(١) د/ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩، ص ١٩٤وما بعدها

والأنظمة المعلوماتية التقنية كأدلة قوية ومؤثرة في الإثبات في القضايا الجنائية(١). ويرجع السبب الرئيسي وراء اعتراف رجال الفقه القانوني بالقيمة الثبوتية للأدلة التقنية الرقمية وإقرار حجيتها في مجال الإثبات الجنائي إلى أن هذه الأدلة تعتمد على قواعد علمية وحسابية دقيقة وقاطعة(٢)، ولا تقبل التأويل أو الشك. وتتميز هذه الأدلة بوضوحها ودقتها في إثبات الصلة بين الجاني والمجني عليه أو بين الجاني والسلوك غير المشروع(٣)، مما يزيد من يقينية تلك الأدلة والمستخرجات لدى محكمة الموضوع(٤). ومن المهم أن يأخذ المشرع المصري في الاعتبار عند صياغة الشروط والمواصفات الواردة باللائحة التنفيذية مجموعة الشروط العامة المتفق عليها في المجتمع الدولي(٥) وأغلب التشريعات الدولية لقبول حجية الدليل الالكتروني(٦).

(١) د/ هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى، مطبعة دار النهضة العربية، الطبعة الأولي، القاهرة، ١٩٩٧، ص٥٣.

(٢) د/ حسن ربيع ، الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية ، القاهرة، ٢٠٠١، ص٧٢٠.

(٣) د/ عائشة مصطفي ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ، المرجع السابق، ص١١٧.

(٤) د/ ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، المغرب، العدد ٣١،١٤٢٧ص١.

(٥) د/ نبيل مدحت سالم ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، ٢٠٠٩، ص٢١٦.

(٦) د/ حاتم بطيخ، دور الانترنت في الإثبات أمام القاضي الجنائي والإداري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٧ ، ص ٦٥٥ وما بعدها

ويمكن تقديم الدليل التقني في الإمارات عن طريق الإجراءات التالية:

١. توثيق الدليل التقني: يتم توثيق الدليل التقني بشكل كامل ودقيق، ويجب أن يتضمن جميع المعلومات والتفاصيل اللازمة لشرح المنتج أو الخدمة التي يتم تقديمها.

٢. توصيف الدليل التقني: يجب توصيف الدليل التقني بشكل مفصل ودقيق، حيث يتم تحديد الأهداف التي يسعى إليها الدليل والمنتجات أو الخدمات التي يتم شرحها.

٣. عرض الدليل التقني للجهات المختصة: يتم عرض الدليل التقني للجهات المختصة في المجال، وذلك للتحقق من صحة ودقة المعلومات المقدمة في الدليل.

٤. اعتماد الدليل التقني: يتم اعتماد الدليل التقني بعد التأكد من صحة ودقة المعلومات المقدمة فيه، وذلك من قبل الجهات المختصة في المجال. ويجب الانتباه إلى أن هذه الإجراءات يمكن أن تختلف قليلاً باختلاف المجال الذي يتعلق به الدليل التقني، ويمكن الحصول على مزيد من المعلومات عن الإجراءات اللازمة من خلال الاتصال بالجهات المختصة. كما ركز القانون الإنجليزي والقانون الأمريكي بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة مسجلة فيه، والتي تزود بشهادة شفوية تكون مقبولة ويتم تقديرها من قبل المحكمة المختصة. وقد قضت محكمة النقض الفرنسية

بأن أشرطة التسجيل الممغنطة التي تكون مدعمة بشهادة شفوية مقبولة تعتبر أدلة قانونية. وتشير المحاكم والتشريعات العالمية إلى أن دلائل الإثبات الرقمية يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي(١). فقد قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان أنه يشترط لقبول سجلات الحاسوب كنسخ حقيقية من السجلات الإلكترونية أن تحتوي على وصف كامل لنظام حفظ السجلات والإجراءات والعمليات المتعلقة بإدخال وتخزين واسترجاع البيانات، لتكون موثوقة بشكل كاف(٢). على النقيض من ذلك، لا توجد في التشريعات العربية المقارنة أية نصوص أو إشارات صريحة تعترف بقيمة وحجية الأدلة المستخرجة من وسائل التقنية بنفس الطريقة التي يفعلها المشرع المصري وأغلب التشريعات الأوروبية. وهذا يتطلب من المشرعين في تلك الدول وضع أسس وآليات وضوابط لقبول هذه الأدلة التقنية في مجال إثبات الجرائم المعلوماتية، ومسايرة التطورات الحاصلة في هذا الشأن(٣).

(١) د/ هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دراسة مقارنة، الطبعة الأولي، دار النهضة العربية، القاهرة، ١٩٩٧، ص ٤٢ وما بعدها.

(٢) د/ علي حسن الطوالبه، مشروعية الدليل الالكتروني المستمد من التفتيش الجنائي دراسة مقارنة، بحث منشور عبر الانترنت، مركز الإعلام الأمني، البحرين، ٢٠٠٩، ص١٨.

(٣) د/ مأمون محمد سلامة، قانون الإجراءات الجنائية ، معلق عليه بالفقه وأحكام النقض، دار الفكر العربي، ١٩٨٠، ص٧٦٠.

تعقيب:

يتضح لنا أن الدليل الرقمي يشير إلى المعلومات الإلكترونية أو البيانات التي تحمل قيمة قانونية في الإثبات، ويمكن للمحاكم الجنائية الاعتماد عليها إذا توفرت الضمانات القانونية المناسبة. ومن المهم تحديث الإطار التشريعي للقوانين المختلفة، وخاصة القانون الجنائي، لتتناسب مع التطورات في نظام الإثبات الجنائي وتطويره، والسماح بالحصول على كافة الأدلة المستخلصة من وسائل الكترونية. ومع ذلك، يجب ضمان مشروعية الدليل المستخلص من وسائل الكترونية أو رقمية، وتجنب الإفراط في استخدامها على حساب حقوق الخصوم. ونظرًا لزيادة استخدام التكنولوجيا الحديثة في الحياة اليومية للأفراد، فإن هذا الأمر أصبح ضروريًا.

الخاتمة

اتضح لنا أن التكنولوجيا لها تأثير كبير على السياسة الجنائية من خلال التغييرات التي تطرأ على قوانين تقنية المعلومات وتطبيقها في المجال الجنائي. فباستخدام التكنولوجيا في الجرائم المعلوماتية يمكن أن نرى تقدمـًا كبيراً في مجال مكافحة الجرائم المعلوماتية، ولكنها في الوقت نفسه تحتاج إلى إطار قانوني واضح ومحدد لضمان عدم انتهاك حقوق الأفراد. وبالتالي، يجب على الدول العمل على تحديث قوانينها لتتوافق مع التكنولوجيا الحديثة وتوفر الحماية اللازمة للمواطنين في العصر الرقمي.

وإذاء ذلك قامت الكثير من الدول إلى تطوير السياسة التشريعية بإدخال نصوص عقابية وإجرائية تتلائم مع ظاهرة الجرائم المستحدثة، ومن هذه القوانين ما كان صائبا كقانون مكافحة جرائم تقنية المعلومات المصري. ومنها ما أصابة القصور، وتعد هذه الدراسة طريقة لمعرفة السياسة التشريعية التي اتبعها المشرع المصري لمواجهة الجرائم التي يتم ارتكابها بواسطة وسائل التقنية الحديثة .

النتائج:

توصل البحث إلى عدة نتائج وتأثيرات للتكنولوجيا على السياسة الجنائية في ضوء قانون تقنية المعلومات، ومن أبرزها:

- تطور الجرائم المعلوماتية وتعقيداتها تتطلب من الدول العمل على تحديث قوانينها لتتوافق مع التكنولوجيا الحديثة وتوفر الحماية اللازمة للمواطنين في العصر الرقمي.

- تقنية المعلومات تساهم في تحسين كفاءة وفعالية العمل الجنائي ومكافحة الجريمة وتسهل عمل القضاة والمحامين في إجراء التحقيقات والتحليلات الجنائية.
- يرتبط استخدام تقنية المعلومات في الجرائم المعلوماتية بمخاطر انتهاك حقوق الأفراد، لذلك يجب على القوانين الجنائية الحديثة أن تحدد حدود استخدام التقنية وتضمن الحماية الكاملة للمواطنين وحقوقهم في الحياة الخاصة والعامة.
- يجب على الدول العمل على تطوير بنيتها التحتية وتعزيز قدراتها التقنية والفنية وتأهيل الكوادر البشرية المختصة بتقنية المعلومات والأمن السيبراني، لتحقيق الاستفادة الكاملة من التكنولوجيا في مجال الجرائم الإلكترونية وحماية المعلومات الحساسة.
- تبين لنا أن التكنولوجيا الحديثة ساهمت في تسهيل العديد من الأمور الحياتية لجميع الأشخاص.
- تبين لنا قيام المشرع المصري بإصدار التشريعات والنصوص الملائمة لمواجهة جرائم تقنية المعلومات والإعتراف بحجية الدليل الجنائي الرقمي.
- تبين لنا أن التشريعات والنصوص التقليدية لا تتلائم مع مواجهة الجرائم المستحدثة من تقنية المعلومات.
- تبين لنا أن جرائم تقنية المعلومات تتسم بالسهولة في ارتكابها والقدرة على إخفاء أثرها وأدلتها.

التوصيات:

- نوصي بتطوير القدرات والتأهيل ورفع كفاءة مأمورى الضبط القضائي وقضاة التحقيق والمحاكمة للتعامل مع التكنولوجيا الحديثة واستخدامها بفعالية في العمل القانوني.
- نوصي بإصدار تشريع جامع مانع خاص بالتكنولوجيا يتضمن الجرائم المستحدثة الناتجة عنها و إعادة النظر في قانون مكافحة جرائم تقنية المعلومات ونص عقوبة مناسبة لكل جريمة من أجل تحقيق الردع العام ولسد الفراغ التشريعي و القانوني، وذلك بإصدار قواعد قانونية ملزمة وصارمة وقواعد تنظيمية، لمسايرة ما يحدث من تطور تكنولوجي.
- نوصي بضرورة التعاون الدولي في مجال مواجهة الجرائم المستحدثة الناتجة عن التكنولوجيا والدعوة إلى إعداد مؤتمر دولي تجتمع حوله دول العالم كافة لوضع إستراتيجية عامة أو شاملة لمواجهة الجرائم المستحدثة أو عقد إتفاقيات ثنائية أو جماعية تتعلق بمكافحة الجرائم الناتجة عن التكنولوجيا الحديثة.
- نوصي بأن يكون هناك قضاة متخصصون في جرائم تقنية المعلومات تكون لهم الخبرة في مجال تكنولوجيا والجرائم الناتجة عنها.

المراجع العربية

المؤلفات العامة:

- د/ أحمد شوقي عمر أبو خطوة، شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، ١٩٩٩.
- د/ أحمد فتحى سرور ، الوسيط فى قانون العقوبات. القسم العام، دار النهضة العربية، القاهرة، ٢٠١٥.
- د/ أحمد فتحى سرور، أصول السياسة الجنائية، دار النهضة العربية، القاهرة، ٢٠١٥م.
- د/ جلال ثروت، نظم القسم العام في قانون العقوبات المصري،، منشأة المعارف، الاسكندرية، ١٩٨٩.
- د/ حسن ربيع ، الإجراءات الجنائية في التشريع المصري ، دار النهضة العربية ، القاهرة، ٢٠٠١.
- د/ حسين محمود ، الوسائل العلمية الحديثة في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٨١.
- د/ خالد الحلبي ، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان ، ٢٠٠٠.
- د/ عمر محمد أبو بكر يونس، الإ جراءات الجنائية عبر الإنترنت في القانون الأمريكي المرشد الفيدرالي الأمريكي لتفتيش نظم الحاسب الآلي وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، دار الفكر العربي، القاهرة،٢٠٠٥.

- د/ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية، الطبعة الأولى، القاهرة، ١٩٩٩.
- د/ سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دار الجامعة الجديدة للنشر، الإسكندرية، ٢٠٠٠.
- د/ مأمون محمد سلامة، قانون الإجراءات الجنائية ، معلق عليه بالفقه وأحكام النقض، دار الفكر العربي ، ١٩٨٠.
- د/ محمد عبد اللطيف فرج، السياسة الجنائية المعاصرة والإتجاهات تطوير القانون الجنائي ودعم التعاون الدولي، الطبعة الأولي ، مطابع الشرطة ، القاهرة، ٢٠١٣.
- د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، الطبعة الثالثة ، ١٩٩٨م.
- د/ نبيل مدحت سالم ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، القاهرة، ٢٠٠٩.
- د/ مصطفى العوجي، دروس العلم الجنائي، مؤسسة نوفل، بيروت – لبنان ، ١٩٨٠.
- د/هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتى، مطبعة دار النهضة العربية، الطبعة الأولي، القاهرة، ١٩٩٧.
- د/ هلالى عبد الله أحمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٩٧.

المؤلفات الخاصة:

- د/ أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الألي، دار النهضة العربية، القاهرة، ١٩٨٢.
- د/ إبراهيم سيد أحمد، الحماية التشريعية لبطاقات الدفع الإلكتروني، الدار الجامعية، الإسكندرية، ٢٠٠٥.
- د/ جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعية المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠١.
- د/ عادل يحي قرني، التحقيق والمحاكمة الجنائية عن بعد، دراسة تحليلية تأصيلية لتقنية ال video conference في المجال الجنائي، الطبعة الأولي، دار النهضة العربية ، القاهرة، ٢٠٠٦.
- د/ عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، دراسة مقارنة في ضوء القواعد العامة للإجراءات الجنائية، الطبعة الأولى، ٢٠٠٩.
- د/ عمر إبراهيم الوقاد، الحماية الجنائية للمعلوماتية، دار النهضة العربية، القاهرة، ١٩٩٩.
- د/ عمر محمد سالم، مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي ، المراقبة الالكترونية والتحقيق الجنائي عن بعد، دار النهضة العربية ، القاهرة، ٢٠١٣م.

- د/ غيث محمد عاطف، قاموس علم الاجتماع، دار المعرفة الجامعية، الإسكندرية، ١٩٩٩.
- د/ فضيل دليو، تكنولوجيا الإعلام والإتصال الجديدة بعض تطبيقاتها التقنية، دار هومة للطباعة والنشر، الجزائر، ٢٠١٢.
- د/ محمد حماد هيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة ، عمان، الطبعة الأولي، ٢٠٠٤.
- د/ محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، ٢٠٠٤.
- د/ محمد سامي الشوا، ثورة المعلومات وإنعكاستها على قانون العقوبات، دار النهضة العربية، القاهرة، ١٩٩٥.
- د/ هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، دار النهضة العربية، القاهرة، ٢٠٠٠.
- د/ هدى حامد قشقوش، جرائم الحاسب الآلي الإلكترونية في التشريع المقارن، دار النهضة العربية، القاهرة، ١٩٩٢.
- د/ هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية ، دار النهضة العربية، ٢٠١٢
- د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الألات الحديثة، القاهرة، ١٩٩٢.

- د/ هشام محمد رستم، جرائم الحاسب المستحدثة، دار الكتب القانونية ، القاهرة، ١٩٩٩.
- د/ هلالى عبد الله أحمد ، حجية المخرجات الكمبيوترية في الإثبات الجنائي ، دار النهضة العربية، القاهرة، ١٩٩٧.

الرسائل العلمية:

- د/ حاتم بطيخ، دور الانترنت في الإثبات أمام القاضي الجنائي والإداري، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٧ .
- د/ ربيع محمود الصغير، القصد الجنائي، دراسة تطبيقية على الجرائم المتعلقة بالانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٥.
- د/ طارق فوزي ، الجوانب الإجرائية في الجرائم المعلوماتية ، رسالة دكتوراة، كلية الحقوق ، جامعة المنوفية، ٢٠١١.
- د/ مروي السيد الحصاوي، مبدأ العالمية في القانون الجنائي، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، ٢٠١٩.
- د/ عائشة مصطفي ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ، دراسة مقارنة ، رسالة ماجستير، كلية الحقوق ، جامعة الإسكندارية ، ٢٠٠٩.

المؤتمرات:

- د/ أشرف عبد الستار، رقمنة الإجراءات الجنائية في ظل جائحة كورونا، بحث مقدم للمؤتمر السنوي الحادي والعشرون مركز البحوث الاجتماعية والجنائية، القاهرة ٢٧ حتى ٢٩/ ٩/ ٢٠٢١م .

- د/ سيف بن عبد الله الجبري، المكتبة الرقمية ودورها في بناء وتطوير مجتمع المعرفة التحديات الاجتماعية والثقافية واللغوية في العالم حاضراً ومستقبلاً، المؤتمر العلمي لكلية الأداب والعلوم الاجتماعية في الفترة ٢-٤ ديسمبر، ٢٠٠٧.
- د/ على محمود على، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية ، أكاديمية شرطة دبي، مركز البحوث والدراسات ، عام ٢٠٠٣.
- د/ عمر الفاروق الحسيني ، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، أعمال المؤتمر السادس الجمعية المصرية للقانون الجنائي، دار النهضة العربية ، ،١٩٩٣.
- د/ كامل السعيد، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنولوجيا، بحث منشور ضمن أعمال المؤتمر العلمي السادس للجمعية المصرية للقانون الجنائي، ١٩٩٣.
- د/ محمد محيي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)،أعمال المؤتمر السادس الجمعية المصرية للقانون الجنائي، دار النهضة العربية،١٩٩٣.
- المؤتمر الدولي لمعهد التخطيط القومي" اقتصاد المعرفة والتنمية المستدامة" الورقة المفاهيمية، القاهرة، ٢٠٢١م.

المجلات العلمية:

- د/ أحمد الهياجنة، مكافحة الجريمة المعلوماتية بالتجريم والعقاب، المجلة الأردنية في القانون والعلوم السياسية ، جامعة مؤتة، الأردن، المجلد الأول، العدد٣، ٢٠٠٩.
- د/ أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، دراسة تحليلية مقارنة ، بحث منشور بمجلة البحوث القانونية والاقتصادية ، العدد ٧٦، ٢٠٢١م.
- د/ أسامة صلاح بهاء الدين، مكانة الإصلاح وإعادة التأهيل في السياسة الجنائية المعاصرة، مجلة الدراسات العليا ، جامعة النيلين، العراق ، المجلد الرابع ، العدد١٦، عام ٢٠١٦م.
- د/ مصطفي أحمد أمين، التحول الرقمي في الجامعات المصرية، كمطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، العدد١٩، ٢٠١٨.
- د / محمد موسي على شحاته، انعكاسات تفعيل آليات التحول الرقمي في ضوء

مبادرات الشمول المالي على تطبيقات الحكومة الإلكترونية بجمهورية مصر العربية ، بحث منشور بمجلة الدراسات المعاصرة، العدد ٩، ٢٠٢٠.

- د/ ناول عبد الهادي، تقييم فعاليات المواجهة التشريعية لجرائم الانترنت، مجلة العدل، المغرب، العدد٣١، ١٤٢٧.

المواقع الإلكترونية:

- استراتيجية مصر الرقمية: منشور على الموقع الالكتروني تاريخ الدخول ٢٧/ ٣/ ٢٠٢٣. mcit.gov.eg.Technology.

المراجع الأجنبية

- Hinings،B.،Gegenhuber،T.،Greenwood، R.،2018.Digital lnnovation and Transformation:An lnstitutional Perspective. Lnformation and Oranization28.
- Liere-Netheler،K.،Packmohr،S.،Vogelsang،K.،2018،Drivers of digital transformation in manufacturing. Ln: Hawaii lnternational Conferece on System Sciences،Waikoloa Beach، Hl.
- MASCALA Corinne،"crimialite et contrat electronique"،IN:Le contrat électronique،Travaux de L'association CAPITANT Henri، jornées national،Paris،2000.
- TOM Forester،Essential problémes to High-tech Society First MIT Prés édition، Cambridge،Massachusetts،1989.
- TGI Pontoise، 6e ch.، 2 février2005: Comm.Com. Electr. 2005، Comm. 35، Ch. Caron: "l'outil exceptionnel de communication et d'échange que représente le réseau internet ne saurait être en tout état de cause une zone de non droit، c'est-à-dire un univers، lieu de liberté où les règles juridiques élémentaires ne s'appliquent pas ".

فهرس الموضوعات

موجز عن البحث ٤٧٦

مقدمة ٤٧٩

المبحث الأول : الأحكام العامة للتكنولوجيا والسياسة الجنائية ٤٨٧

المطلب الأول : مفهوم التكنولوجيا ٤٨٨

المطلب الثاني : مفهوم السياسة الجنائية ٤٩٢

المطلب الثالث : الفرق بين التكنولوجيا والسياسة الجنائية ٤٩٦

المبحث الثاني : ملامح تطوير السياسة التشريعية في ضوء قانون تقنية المعلومات .. ٤٩٩

المطلب الأول: المواجهة التشريعية لجرائم تقنية المعلومات ٥٠٠

المطلب الثاني : تطور قواعد الاختصاص والقانون الواجب التطبيق ٥٠٦

المطلب الثالث : حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية ٥١٧

الخاتمة ٥٣١

المراجع العربية ٥٣٤

المراجع الأجنبية ٥٤٢

فهرس الموضوعات ٥٤٣