

## تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية (وقائع ومقاربات)

The development of international legislations and conventions in the  
field of informatics crimes ( facts and approaches )

Le développement de législations et de conventions internationales  
dans le domaine des crimes informatiques (faits et approches)

تاريخ إرسال المقال : 03/04/2018 تاريخ قبول المقال للنشر : 04/06/2018

د. سعيداني سلامي / جامعة محمد بوضياف - المسيلة

### ملخص :

اختلفت المظاهر الإجرامية لظاهرة الجريمة المعلوماتية وتباينت أنواعها، فلم تعد تهدد العديد من المصالح التقليدية التي تحميها القوانين والتشريعات العادية منذ عصور قديمة، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات والمعلومات.

فالجريمة المعلوماتية تعتبر من بين الظواهر الحديثة، نضيرارتباطها بتكنولوجيا حديثة هي تكنولوجيا المعلومات والاتصالات. وقد أحاط بتحديد الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية لوضع تعريف جامع مانع لها ولكن الفقه لم يجتمع على وضع تحديد محدد لها بل أن البعض ذهب إلى ترجيح عدم وضع هذا التحديد بحجة أن هذا النوع من الإجرام ما هو إلى جريمة تقليدية ترتكب بأسلوب إلكتروني.

وعلى أية حال، فإنه على الرغم من تزايد الجهود الدولية، الإقليمية والوطنية في التصدي لظاهرة الإجرام المعلوماتي إلا أنه لا يوجد تحديد محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية، فقد ذهب جانب من الفقه إلى تناولها بالتعريف المدقق على نحو ضيق وجانب آخر عرفها على نحو موسع.

لذا يأتي هذا المقال ليشرح و يفسر تلك المواد القانونية الوطنية والإقليمية و كذا التشريعات الدولية لظاهرة الجرائم المعلوماتية.

الكلمات المفتاحية: التشريع، التشريع الدولي، الاتفاقيات، الجريمة، الجريمة المعلوماتية .

### Abstract:

The criminal manifestations of the phenomenon of cybercrime differed and did not threaten many of the traditional interests protected by ordinary laws and legislations since ancient times. They also threatened many of the legal interests and centers developed by IT after the combination of communications and information revolutions.

The crime of informatics is one of the modern phenomena, bad link with modern technology is information and communication technology. The definition of informational crime has been characterized by a lot of ambiguity, as there have been many efforts to develop a comprehensive definition that contradicts it. However, jurisprudence has not met a specific definition. Some have even suggested that this definition should not be made on the grounds that this type of crime is a traditional crime committed in an electronic manner .

However, despite increasing international, regional and national efforts to address the phenomenon of cybercrime, there is no specific and agreed definition among cybercriminals on the concept of cybercrime. A part of the jurisprudence went to a narrowly defined definition, Towards an expanded.

So this article explains and explains these national and regional legal articles and international legislation on the phenomenon of cybercrime.

**Keywords:** legislation, international legislation, conventions, crime, information crime.

### Résumé:

Différentes manifestations criminelles du phénomène de la criminalité cybernétique et divers types, ne menacent plus grand nombre des intérêts traditionnels protégés par les lois et la législation normale depuis les temps anciens, mais a menacé plusieurs des intérêts et des centres juridiques développés par la technologie de l'information après les communications combinées et de l'information.

Le crime de l'informatique est l'un des phénomènes modernes, les technologies de l'information et de la communication étant un mauvais lien avec la technologie moderne. Il a fallu identifier la cybercriminalité beaucoup d'ambiguïté où il y avait beaucoup d'efforts pour développer un esprit avec une définition inclusive mais Fiqh ne se rencontrent à un particulier les identifier, mais certains sont allés à la

probabilité de ne pas mettre cette limitation au motif que ce type de crime est un crime traditionnel commis d'une manière lettre.

Cependant, malgré les croissants, les efforts régionaux et nationaux et internationaux dans la lutte contre le phénomène de la criminalité d'information, mais il n'y a pas d'identification spécifiée et convenue entre les chercheurs sur le concept de la cybercriminalité, le côté est allé jurisprudence à traiter par vérificateur .définition étroite et avec un autre connu Vers un élargi

Cet article explique et explique ces articles juridiques nationaux et régionaux .et la législation internationale sur le phénomène de la cybercriminalité

**Mots-clés:** législation, législation internationale, conventions, criminalité, . criminalité informationnelle

#### مقدمة:

إن التشريعات القانونية التي تصدت لجرائم المعلومات وغيرها من التشريعات المشابهة، أو تشريعات حماية الحياة الخاصة أو الخصوصية أو تشريعات الملكية الفكرية التي تصدت لحماية المصنفات الرقمية، أو تشريعات خاصة بحماية استخدام الحاسب أو تعديل لقوانين العقوبات القائمة، إنما جاء من أجل حفظ الحياة البشرية وتنظيم سلوكياتها في البيئة الرقمية التي تتسم بالإهمام والغموض والكثير من الأحيان تتميز التعقد.

أمام الخصائص المميزة لجرائم الحاسوب المتعددة والمختلفة، وأمام مشكلاتها وتحدياتها المتزايدة في ظل البيئة الجديدة للإعلام والاتصال، وأمام اتجاهات العمل الدولي العالمي والإقليمي بشأن سياسات مكافحتها، اتجه عدد من الدول، إلى وضع تشريعات خاصة أو تعديل قوانين العقوبات لديها بغية تجريم جرائم الكمبيوتر والانترنت (الجرائم المعلوماتية)، وقد جاء اتجاه التشريع المقارن في التعامل مع جرائم الحاسوب متفقاً مع ذات الاتجاهات التي اختطتها المنظمات الإقليمية والدولية.

إذا كان الاهتمام الدولي بإخطار استخدام الحواسيب وبنوك المعلومات على الحياة الخاصة قد انطلق في السبعينات، فإن نفس الحقبة شهدت ولادة العديد من تشريعات حماية الخصوصية، وإذا كانت الثمانينات قد شهدت جهوداً فاعلة في حماية استخدام الحاسوب والتصدي الدولي لمشكلات جرائم الحاسوب فإن الحقبة ذاتها شهدت سن العديد من قوانين حماية استخدام الحاسوب أو وضع نصوص خاصة بشأن ذلك كتعديل على قوانين العقوبات، وذات الحقبة أيضاً شهدت اتجاهاً متزايداً بشأن حماية برامج الحاسوب بتشريعات الملكية الفكرية، وبفعل الطبيعة الخاصة لمعطيات الحاسوب من حيث كونها غير مادية، وبفعل ما أثاره التطبيق القضائي لنصوص القوانين الجنائية على جرائم الحاسوب من مشكلات، ولضمان عدم إفلات الجناة من العدالة لعدم كفاية القوانين أو عجزها عن الانطباق على هذه الجرائم المستحدثة، وصونا لمبدأ الشرعية الذي يقضي بأن لا جريمة ولا عقوبة بغير نص قانوني، وفي

ظل هذا المبدأ نحاول في هذه الورقة العلمية عرض المعالم الرئيسية الشاملة لهذه التشريعات، لتوضيح مسالك القانون بشأن الجرائم المعلوماتية.

## 1. ثلاثية الجريمة (المعلوماتية/ الإلكترونية/ الحاسوب): مدخل تفسيري عام

### 1.1. تعريف الجريمة المعلوماتية:

تعددت الآراء بشأن تعريف الجريمة الإلكترونية ، كل رأي تبني مفهوماً بالنظر إلى الزاوية التي رآها ، فهناك جانب من الفقه عرفها من زاوية فنية، وأخرى قانونية ، وهناك جانب آخر يرى تعريفها بالنظر إلى وسيلة ارتكابها أو موضوعها أو حسب توافر المعرفة بتقنية المعلومات لدى مرتكبها أو استناداً لمعايير أخرى حسب القائلين بها<sup>1</sup> ، وهذا ما حدا بالأمم المتحدة - مدونتها بشأن الجريمة المعلوماتية - إلى عدم التوصل لتعريف متفق عليه دولياً ، ولكن ورغم صعوبة وضع تعريف لظاهرة هذه الجريمة وحصرها في مجال ضيق ، إلا أن مكتب تقييم التقنية في الولايات المتحدة الأمريكية عرفها من خلال تعريف الحاسب الآلي بأنها « الجرائم التي تقوم فيها بيانات الحاسب الآلي والبرامج المعلوماتية بدور رئيسي » ، كما عرفت أيضاً بأنها « نشاط جنائي يمثل اعتداءً على برامج وبيانات الحاسب الإلكتروني » ، وعرفت أيضاً بأنها « كل استخدام في صورة فعل أو امتناع غير مشروع للتقنية المعلوماتية ، ويهدف إلى الاعتداء على أي مصلحة مشروعة ، سواء أكانت مادية أو معنوية » .

### 2.1. الجريمة الإلكترونية:

يختلف موضوع الجريمة الإلكترونية بحسب الزاوية التي ينظر إليها منه ، فمن ناحية قد يكون الحاسب الآلي أو المعلومات المخزنة فيه موضوعاً للجريمة ، ومن ناحية أخرى قد يكون فيها الحاسب الآلي أداة للجريمة الإلكترونية ووسيلة تنفيذها.

#### أولاً: الحالة التي يكون فيها الحاسب الآلي أو المعلومات

#### المخزنة فيه موضوعاً أو محلاً للجريمة :

في هذه الحالة وهي ما يطلق عليها البعض ( أداء سلبية ) ، يكون هناك صورتان للاعتداء ، اعتداء واقع على المكونات المادية للحاسب الآلي ذاته كالأجهزة والمعدات ، والتي تتمثل في جرائم سرقة أو إتلاف شاشة الحاسب أو شبكة اتصالاته الخاصة أو آلة الطباعة<sup>2</sup> ، ومن ناحية أخرى قد يكون الاعتداء موجهاً إلى مكونات الحاسب الآلي غير المادية كالبيانات والبرامج مثل جرائم الاعتداء على البيانات المخزنة في ذاكرة الحاسب الآلي أو البيانات المنقولة عبر شبكات الاتصال المختلفة والتي تتمثل في جرائم السرقة أو الإتلاف أو التقليد أو محو أو تعطيل هذه البيانات ، والصورة الثانية تمثل الاعتداء ذاته موجهاً إلى برامج الحاسب الآلي من خلال تزوير المستخرجات الإلكترونية وإفشاء محتوياتها وهو ما اصطُح على تسميته ( سرقة ساعات الحاسب الآلي )<sup>3</sup> . ومن نافلة القول أن النوع الأخير من الاعتداءات تعجز حياله نصوص قانون العقوبات الحالية - التي قننت في ظل تفكير يقتصر إدراكه على المال الملموس والمستندات ذات الطبعة المادية - عن احتوائه واستيعابه نظراً لأن محل هذه الاعتداءات مال غير مادي ( معنوي ) ذو طابع خاص ، أي أنه في صورة أخرى غير صورة المال بمفهومه الجنائي التقليدي .

ثانيا : حالة يكون فيها الحاسب الآلي أداة لارتكاب الجريمة ووسيلة تنفيذها :  
ففي هذه الحالة والتي يطلق عليها البعض ( أداة إيجابية ) يستخدم الجاني الحاسب الآلي في ارتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات ، وذلك عن طريق التلاعب في الحاسب ، وكذلك النظام المعلوماتي بصفة عامة ، وفي هذه الحالة نكون بصدد جرائم تقليدية بحتة.<sup>4</sup>

### 3.1. الجرائم الحاسوبية (جرائم الحاسوب)

بعض الدراسات والنشاطات العلمية اتجهت إلي تبني منهج يقوم علي تصنيف النشاطات المتعلقة بالحاسب الآلي إلي فئات وأنواع بمثابة مفترض وضروري لهذا الموضوع .  
وطبقا لهذا المعني فإن الكاتب دون بيكر (Donn Parker) ردَّ أشكال إساءة الحاسب الآلي إلي أنماط أو أشكال يتميز كل منها بالدور الذي يلعبه هذا الحاسب ذاته، وهكذا فإن الحاسب الآلي لا يعدو أن يقوم بأحد الأدوار التالية : دور الضحية في الجريمة ؛ دور المحيط أو البيئة التي ترتكب فيها الجريمة؛ دور الوسائل التي ترتكب بواسطتها الجريمة، ودور التخويف أو الخداع أو غش الضحية.<sup>5</sup>

وبعض آخررد الأنشطة التي بالحاسب و التي يمكن أن تعتبر أنشطة غير مشروعة إلي الفئات الرئيسية هي : غش الحاسب الآلي ؛ إتلاف المعطيات(البيانات) أو البرامج ؛ سرقة المعلومات .

ورغم الفارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الإنترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به ، فإن جرائم الإنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية ، إلا أن الواقع التقني أدى إلى اندماج الميدانين ( الحوسبة والاتصالات ) وظهور مصطلح (Cybercrime).

### 4.1. أنواع الجرائم المعلوماتية

أ- جرائم الحاسب الآلي : ويقصد بها الأفعال التي تشكل اعتداء على أجهزة الحاسب الآلي، سواء على مكوناته المادية ( Hardware ) كوحدات الإدخال والإخراج ، ووسائل التخزين المرنة والصلبة أو الشاشة و الطابعة أو على مكوناته المعنوية (Software data bases) كالبيانات والمعلومات المخزنة داخل الحاسب الآلي ، وعلى ذلك فإن جرائم الحاسب تختلف حسب طبيعة الشيء محل الاعتداء ، فالاعتداء أحيانا يقع على أدوات وآلات الحاسب الآلي وأحيانا أخرى يقع على برامج ومعلومات داخل الحاسب الآلي ، وفي كلتا الحالتين فإن الحاسب ومحتوياته هو هدف السلوك الإجرامي.

ب- جرائم الإنترنت : وهي كل فعل غير مشروع يقع على المواقع بقصد تعطيلها أو تشويهها أو تعديلها والدخول غير المشروع لمواضع غير مصرح بالدخول إليها، واستخدام عناوين غير حقيقية للدخول في شبكة المعلومات واقتحام الشبكات ونقل الفيروسات، وإرسال الرسائل بكافة أنواعها عبر البريد الإلكتروني كالماسة بكرامة الأشخاص أو المستهدفة ترويج مواد أو

أفعال غير مشروعة .

ج- جرائم شبكة المعلومات : وهي كل فعل غير مشروع يقع على وثيقة أو نص موجود بالشبكة ومن أمثلته انتهاك الملكية الفكرية للبرامج و الإنتاج الفني و الأدبي و العلم، و ارتكاب هذه الجرائم عبر شبكة المعلومات يتطلب اتصال بالانترنت واستخدام الحاسب الآلي للوصول إلى قواعد البيانات للاطلاع عليها أو تغييرها .

د- الجرائم المتعلقة باستخدام الحاسب الآلي : وهي الجرائم التي يكون الحاسب الآلي وسيلة لارتكابها كالاختيال و التزوير بواسطة الحاسب، ولقد كانت هذه الجريمة مندمجة في جرائم الحاسب الآلي وتعتبر جزء منها، إذ كان مصطلح جرائم الحاسب يستخدم للدلالة على كل صور جرائم الحاسب الآلي سواء أكان الحاسب هدفا صريحاً للفعل الإجرامي أو وسيلة له، إلا أنه بعد اتساع جرائم الحاسب وولادة جرائم الانترنت أصبح مصطلح الجرائم المتعلقة بالحاسب الآلي يعتبر من الجرائم التي يكون الحاسب وسيلة لارتكابها، أي أنها كل فعل غير مشروع يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية.<sup>6</sup>

2. بماذا تتميز الجريمة المعلوماتية عن غيرها من الجرائم؟

رغم أن الورقة العلمية يدور حول نطاق تطبيق نصوص القانون الجنائي، إلا أنه وكما يبدو أننا بصدد ظاهرة إجرامية ذات طبيعة متميزة تتعلق غالباً بما يسمى بالقانون الجنائي المعلوماتي.

ففي معظم حالات ارتكاب الجريمة المعلوماتية نجد أن الجاني يتعمد التدخل في مجالات النظام المعلوماتي المختلفة ومنها:

### 1.2. مجال المعالجة الإلكترونية للبيانات:

يتدخل الجاني من خلال ارتكاب الجريمة المعلوماتية في مجال المعالجة الإلكترونية الآلية للبيانات سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسوب وذلك بغرض الحصول على معلومات.

### 2.2. مجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية.

يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات وهي طريقة أوتوماتيكية تمكن مستخدم الحاسوب من كتابة الوثائق المطلوبة بدقة متناهية بفضل الوسائل التقنية الموجودة تحت يده وبفضل إمكانيات الحاسوب، من تصحيح وتعديل ومحو وتخزين وطباعة واسترجاع وطباعة وهي إمكانيات لها علاقة وثيقة بارتكاب الجريمة، إذ ينبغي ألا ننسى من أننا نتعامل مع مفردات جديدة كالبيانات والبرامج.

وظاهرة الجريمة المعلوماتية تهتم بصفة خاصة بالمجال المصرفي، وتفتح هذه الثورة المعلوماتية مجالاً جديداً لخلق أدوات جديدة في المعاملات التجارية، فإذا كان التعامل والإثبات ينحصر في المستند الورقي، فإنه أصبحت الآن تسجيلات إلكترونية ومحركات إلكترونية أو سند شحن، وكذلك فإن المستخرجات لها قيمة في الإثبات، بجانب المستند الورقي. ويشهد الواقع العملي تقدم مذهل في عالم اليوم نحو الاعتماد على الوسائل الحديثة في الإثبات إذ كان ذلك

لا يمنع من وجود وسائل الإثبات التقليدية بشرط أن ينظم المشرع الحديث هذه المسائل من خلال نصوص تشريعية<sup>7</sup> تعالج هذا الأمر، وبالمثل فإن الجريمة المعلوماتية تتعلق بكل سلوك غير شرعي أو غير مسموح به نحو الولوج إلى المعالجة الآلية للبيانات أو نقلها، ومن ثمة فإن هذه المعالجة غير الشرعية تجعلنا في صدد القانون الجنائي والتي تعتبر معظم نصوصه التقليدية عاجزة عن مواجهة هذا التطور التكنولوجي والمعلومات.<sup>8</sup>

### 3. مظاهر الجريمة المعلوماتية

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة ، وتعدد صور الجرائم التقليدية موجهة أخرى ، فإن ذلك لا يعني تناول هذا الموضوع بالطريقة المدرسية التقليدية التي تتمثل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تثير مشكلة في تطبيق النصوص القانونية إما لتعذر المطابقة بينها وبين النصوص التقليدية أو بسبب الفراغ التشريعي لمواجهة هذه الجرائم ، ولما كان المجال لا يتسع للحديث عن كل أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها إثارة للمشكلات القانونية وهي جرائم الاعتداء على الحياة الخاصة و جرائم الأموال وجريمة التزوير.

#### أولاً: جرائم الاعتداء على الحياة الخاصة للأفراد

المقصود من التطرق لموضوع جرائم الاعتداء على الحياة الخاصة للأشخاص التعرض لتلك الجرائم التي يتعذر علينا مواجهتها بالنصوص التقليدية ، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك ومناقشة الحالات التي تثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم وهي جرائم الاعتداء على الحياة الخاصة.

يصعب بداية حصر عناصر الحق في الحياة الخاصة فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية.<sup>9</sup>

أما علاقة الحياة الخاصة بالتقنية المعلوماتية فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية.

هكذا أصبحت الشبكات المعلوماتية مستودعا خطيرا للكثير من أسرار الإنسان التي يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يدلي بها بعض الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك و المؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها ، فالبيانات الخاصة بشخصية المستخدم يمكن الوصول إليها عن طريق زيارة بعض المواقع على شبكة المعلومات، لان شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الأجهزة

وتسمى هذه البروتوكولات الخاصة مثل بروتوكولات HITP الذي يمكن عن طريقها الوصول إلى رقم جهاز الحاسب الشخصي ومكانه وبريده الإلكتروني، كما أن هناك بعض المواقع التي يؤدي الاشتراك في خدماتها إلى وضع برنامج على القرص الصلب للحاسب الشخصي وهو ما يسمى cookies وهدفه جمع معلومات عن المستخدمين، بل إن أخطارها في استخدام هذه الشبكة يتمثل في إن كل ما يكتبه الشخص من رسائل يحفظ في أرشيف خاص يسمح بالرجوع إليه ولو بعد عشرون عاماً<sup>10</sup>. ويظن الكثيرون إن الدخول باسم مستعار أو بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة فإن مزود الخدمة أو internet service provider (ISP) يمكنه الوصول إلى كل هذه المعلومات بل ويمكنه أيضاً معرفه المواقع التي يزورها العميل.

وعليه فإن القوانين المقارنة اهتمت بهذه المسألة واتجهت إلى تبني العديد من الضمانات التي يمكن تلخيصها في:

1- مبدأ الأخطار العام: وهو أن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومات التي تقوم بتسجيلها فيجب أن تكون هناك قيود على إنشاء الأنظمة المعلوماتية المختلفة لمعالجة البيانات<sup>11</sup>.

2- شرعية الحصول على المعلومة: يجب أن يتم الحصول على المعلومة بطريقة تخلو من الغش والاحتيال حيث تمنع المادة 25 من القانون الفرنسي للمعلوماتية تسجيل أي معلومة إلا إذا كانت برضاء صاحب الشأن.

3- التناسب بين المعلومات الشخصية المسجلة والهدف من ذلك التسجيل، فعلى الجهة الراغبة في إقامة أي نظام معلوماتي أن تحدد الهدف من إقامته<sup>12</sup>.  
تجدر الإشارة أيضاً إلى معاهدة بودابست لسنة 2001 التي تهدف إلى توحيد الجهود الدولية لمكافحة جرائم الكمبيوتر والتي تضمنت العديد من التعريفات للأفعال المجرمة تاركة لكل دولة تحديد العقوبة التي تراها مناسبة للفعل.

فنصت المادة 2 منها على تجريم الدخول غير المشروع illegal access إلى أي نظام معلوماتي، ونصت المادة 3 منها على أن تجرم الدول الأعضاء كل اعتراض لهذه البيانات بأي وسيلة إلكترونية دون وجه حق، أما المواد 4- وما بعدها فنصت على تجريم أي تعديل في البيانات أو تحريفها أو تدميرها أو تعديلها أو تغيير مسارها، كما نصت المادة 5 على تجريم التدخل في النظام المعلوماتي والعمليات المنطقية ونصت المادة 6 على إساءة استخدام النظام المعلوماتي بشكل يؤدي إلى إفشاء نظم الحماية الخاصة به دون وجه حق.

#### ثانياً: جرائم الاعتداء على الأموال

إذا كان الركن المادي للسرقة المتمثل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرع شكل السلوك الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسب لجريمة

النصب حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الأخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة والاحتيال التي ترتكب عن طريق التقنية المعلوماتية؟ لذا سوف نعرض إلى الوسائل الفنية التي يتم عن طريقها الاختلاس قبل عرض تكييفها القانوني:

#### - الوسائل الفنية للتحويل الإلكتروني للأموال:

1. يتم التحويل غير المشروع للأموال بعدة وسائل يصعب حصرها لسرعة وتيرة التطور في هذا المجال لكن يمكن الإشارة إلى أكثرها انتشاراً.
1. استخدام برامج معده خصيصا لتنفيذ الاختلاس: أشهر هذه الوسائل هو تصميم برامج معينة تهدف إلى إجراء عمليات التحويل الآلي من حساب إلى آخر سواء كان ذلك من المصرف نفسه أو من حساب آخر في مصرف آخر على أن يتم ذلك في وقت معين يحدده مصمم هذا البرنامج<sup>13</sup>.
2. التحويل المباشر للأرصدة: يتم ذلك عن طريق اختراق أنظمة الحاسب وشفرات المرور.
3. التلاعب بالبطاقات المالية: لقد ظهرت أولى هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية Electronic Banking والنقود المالية digital Cash .
4. جرائم الاعتداء على أجهزة الصرف الآلي للنقود: تثار هذه المشكلة في حالة استخدام الجهاز لصرف ما يتجاوز الرصيد الفعلي اذا تم ذلك بواسطة العميل صاحب البطاقة فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة طبقاً للمادة 444ع لان الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما إن هذه الأخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.
5. جرائم الاستيلاء على النقود الإلكترونية: يمكن تعريف النقود الإلكترونية Electronic Cash بأنها "قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير من قام بإصدارها، وتستعمل كأداة دفع". وتتمثل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الائتمانية، لأن النقود الإلكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود.<sup>14</sup>

#### 4. زوايا مظاهر الجريمة المعلوماتية

يختلف موضوع الجريمة المعلوماتية بحسب اختلاف الزاوية التي ينظر فيها إزاء الإعتداء الموجه ضد أحد مكونات النظام المعلوماتي، فمن ناحية قد يكون هذا الأخير نفسه موضوع للجريمة المعلوماتية، ومن ناحية قد يكون النظام المعلوماتي هو وسيلة للجريمة المعلوماتية

وأداة تنفيذها.

#### 1.4. كون النظام المعلوماتي موضوعاً للجريمة المعلوماتية.

في هذه الحالة إن جرائم المعلوماتيات بمعناها الفني التي تتفق مع الجرائم التقليدية البحثية، فمن ناحية نجد أن مجل الجريمة المعلوماتية في حالة وجود اعتداء على المكونات المادية للنظام المعلوماتي (كالأجهزة والمعدات المعلوماتية وغيرها) يتمثل في جرائم سرقة أو إتلاف هذه المكونات والمتمثل في الحاسبات أو شاشات أو شبكة الاتصال الخاصة أو حتى آلات الطبع المرفق بها.<sup>15</sup>

من ناحية أخرى، إذا كان الإعتداء موجه إلى مكونات غير مادية للنظام المعلوماتي، (كالبيانات والبرامج) مثل جرائم الإعتداء على البيانات المخزنة في ذاكرة الحاسوب أو البيانات المنقولة عبر شبكات الاتصال المختلفة والتي تتمثل في جرائم السرقة أو التقليد أو الإتلاف أو محو وتعطيل هذه البيانات، أو كان الإعتداء ذاته موجه إلى برامج الحاسوب من خلال تزوير المستخرجات الإلكترونية وإفشاء محتوياتها وما اصطلح على تسميته «بسرقة ساعات عمل الحاسوب».

#### 2.4. كون النظام المعلوماتي هو أداة الجريمة المعلوماتية ووسيلة تنفيذها.

ففي هذه الحالة، ليس هناك أدنى شك أننا بصدد جرائم تقليدية، يكون فيها النظام المعلوماتي أو جهاز الحاسب الآلي هو أداة ارتكاب الجريمة المعلوماتية ووسيلة تنفيذها، ومن هذه الناحية، نجد أن الجاني يمكن استخدام الحاسب الآلي لارتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات المعلوماتية، وذلك عن طريق التلاعب في الحاسوب وكذلك النظام المعلوماتي بصفة عامة.<sup>16</sup>

#### 5. الاتفاقيات الدولية والعربية الضامنة من الجرائم المعلوماتية

##### 1.5. الاتفاقيات الدولية للجرائم المعلوماتية

تعد المعاهدات الدولية هي الأساس الذي يرتكز عليه التعاون الدولي في مجال مكافحة الجرائم الإلكترونية وقد تم عقد العديد من المعاهدات التي تعمل على التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ومن تلك المعاهدات معاهدة بودابست والمعاهدة الأوروبية، معاهدة برن، معاهدة تريبس.

##### أولاً: معاهدة بودابست لمكافحة جرائم الإنترنت

شهدت العاصمة المجرية بودابست في أواخر عام 2001 ميلاد أولى المعاهدات الدولية التي تكافح جرائم الإنترنت وتبلور التعاون والتضامن الدولي في محاربتها، ومحاولة الحد منها خاصة بعد أن وصلت تلك الجرائم إلى حد خطير أصبح يهدد الأشخاص والممتلكات.<sup>17</sup> وبعد التوقيع على تلك المعاهدة الدولية، التي تهدف إلى توحيد الجهود الدولية في مجال مكافحة جرائم الإنترنت والتي انتقلت من مرحلة ابتدائية كانت تتمثل في محاولات التسلل البريئة التي كان يقوم بها هواة في الأغلب الأعم من الحالات ودون أي غرض إجرامي إلى مرحلة جديدة يقوم بها محترفون على أعلى درجة من التخصص، وتتمثل في الاحتيال والاختلاس وجرائم

تهديد الحياة، وهي قضايا تعرض حياة وممتلكات الكثير من رواد شبكة الإنترنت للخطر، - هو الخطوة الأولى في مجال تكوين تضامن دولي مناهض لتلك الجرائم التي تتم على شبكة الإنترنت واستخدامها الاستخدام الأسوأ ويعد التوقيع على تلك الإتفاقية- من المسؤولين في الدول الأوروبية إضافة إلى أمريكا واليابان وكندا وجنوب إفريقيا، هونتا مباحثات ومفاوضات استغرقت أكثر من أربعة أعوام حتى يتم التوصل إلى الصيغة النهائية المناسبة لتلك الإتفاقية حتى يتم التوقيع عليها من جميع الأطراف دون أن تجد أي اعتراض من أي منهم بل على العكس لتجد القبول من أطراف جدد ليتم توسيع دائرة الدول التي توافق على الانضمام إلى تلك الإتفاقية ويتم توسيع الإتحاد الدولي والتضامن الدولي في مجال مكافحة جرائم الإنترنت.<sup>18</sup>

### ثانياً: المعاهدة الأوروبية لمكافحة جرائم الانترنت

وقعت اللجنة الخاصة المعنية بقضايا الجريمة بتكليف من المجلس الأوروبي على المسودة النهائية لمعاهدة شاملة تهدف لمساعدة البلدان في مكافحة جرائم الإنترنت وسط انتقادات من دعاة حماية الحرية الشخصية، وبعد أن يتم المصادقة عليها من قبل رئاسة المجلس وتوقيعها من قبل البلدان المعنية ستلزم الإتفاقية الدول الموقعة عليها بسن الحد الأدنى من القوانين الضرورية للتعامل مع جرائم التقنية العالية بما في ذلك الدخول غير المصرح به إلى شبكة ما والتلاعب بالبيانات وجرائم الاحتيال والتزوير التي لها صلة بالكمبيوتر وصور القاصرين الإباحية وانتهاكات حقوق النسخ الرقمي.

وتتضمن بنود المعاهدة التي تم تعديل مسودتها 27 مرة قبل الموافقة عليها فقرات تكفل للحكومات حق المراقبة وتلزم الدول بمساعدة بعضها البعض في جمع الأدلة وفرض القانون لكن الصلاحيات الدولية الجديدة ستكون على حساب حماية المواطنين من إساءة الحكومات استخدام السلطات التي أعطتها لهم تلك الإتفاقية التي قد يسيئون استعمالها.<sup>19</sup>

### ثالثاً: معاهدة برن لحماية المصنفات الأدبية والفنية

تعتبر معاهدة برن التي تم التوقيع عليها في عام 1971 في سويسرا هي حجر الأساس في مجال الحماية الدولية لحق المؤلف وقد وقعت على هذه الإتفاقية 120 دولة من بينها جمهورية مصر العربية وتعد المادة التاسعة من تلك الإتفاقية هي أساس في تلك الإتفاقية لأنها تنص على منح أصحاب حقوق المؤلف حق استثنائي في التصريح بعمل نسخ من هذه المصنفات بأي طريقة وبأي شكل كان.

وفضلاً عن ذلك، تمنح اتفاقية برن صاحب الحق المؤلف الحق في أن يرخص أو يمنع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذا تلزم الإتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنياً أم أجنبياً.

ويرجع الاهتمام بحق المؤلف إلى أنه الوسيلة القانونية الرئيسية لحماية حقوق المؤلفين، فحق المؤلف من أهم الحقوق التي تكفلها النظم القانونية على اختلافها للمبدعين والمؤلفين حماية لإبداعاتهم الفكرية، إن لم يكن أهمها على الإطلاق، ويوفر هذا الحق -بشروط معينة- لمؤلفي مصنفات معينة في الآداب والفنون والعلوم، أي كان نوع هذه المصنفات، أو أهميتها،

أو طريقة التعبير عنها، أو الغرض من تصنيفها، حماية قانونية لا بأس بها، لمدة زمنية معينة، وتنظيم هذه الحقوق في مصر وكافة الدول العربية بمقتضى تشريعات تكاد تتشابه أحكامها تقريبا، كما تستند في مجملها إلى اتفاقية برن لحماية المصنفات الأدبية والفنية التي أبرمت في 9 سبتمبر 1886 وهي أول اتفاقية دولية لحماية حق المؤلف، المعدلة في باريس عام 1971. ومن أهم الاتفاقيات الثمانية والعشرين التي وقعت عليها الدول الموقعة على اتفاقية الجات، الإتفاقية المعروفة باسم اتفاقية المجالات المتعلقة بالتجارة في حقوق الملكية الفكرية، وأهم ما تضمنته في نظرنا أنها أعطت لموضوع الملكية الفكرية بشكل عام بعدا عالميا مهما<sup>20</sup>، وربطت موضوعات الملكية الفكرية بآليات دولية محددة قد لا تستطيع دول كثيرة الفكاك منها، ولأن يكون لهذه الإتفاقية تأثيرات مهمة سواء على اقتصاديات كثير من الدول ومنها الدول العربية أو على تشريعاتها الوطنية، ومن الموضوعات التي تناولتها هذه الإتفاقية تناولا صريحا موضوع الحماية القانونية لبرامج الكومبيوتر.

#### رابعاً: معاهدة تريبس

معاهدة تريبس هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطوع عليها خصوصا مع انتشار عمليات السطوع الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية.

وتلك الإتفاقية تم التوقيع عليها من قبل الدول الأعضاء بها عام 1994 وقد عالج موقعوا الإتفاقية العامة للتعريفات والتجارة (الجات) حقوق الملكية الفكرية بين المعايير الدولية والمعايير المحلية وتتضمن تلك الإتفاقية العديد من الإجراءات الهامة والفعالة لردع الاعتداءات على حقوق الملكية الفكرية، كما أنها ومن جهة أخرى، تفرض على الدول اتخاذ العديد من التدابير الهامة لمعالجة الوضع، ومن تلك التدابير على سبيل المثال لا الحصر إعطاء الحق للسلطات في إصدار الأوامر بشن حملات مفاجئة لضبط أدلة ارتكاب الجريمة والتي عادة ما تكون سهلة التخلص منها لولم تكن هناك سرعة في محاولة ضبطها وكذلك التحفظ على أدوات ارتكاب الجرائم وذلك فضلا عن فرض عقوبات جنائية رادعة.<sup>21</sup>

#### 2.5. الاتفاقيات العربية للحماية من الجرائم المعلوماتية

في نطاق الدول العربية، نجد أن البعض منها أيضا قد حذا حذو الدول السابقة وهي المملكة العربية السعودية وفقا للتشريع رقم 11 الصادر في 17 ديسمبر 1989، ومصر وفقا للتعديل الصادر في 4 يونيو سنة 1992 بالتشريع رقم 38 لسنة 1992 المعدل للتشريع رقم 354 لسنة 1954، والإمارات بالتشريع الاتحادي رقم 40 لسنة 1992 الصادر في 28 سبتمبر سنة 1992 والأردن بتشريعيها رقم 22 لسنة 1992، الصادر في ديسمبر سنة 1992 وتونس بتشريعيها رقم 36 الصادر في 24 فبراير سنة 1994.<sup>22</sup>

لكن في ظل ما سبق فهل تمكنت النظم القانونية العربية من التقاطع مع موجات التشريع في حقل تقنية المعلومات؟ هل تقاربت مع التدابير التشريعية لعصر تقنية المعلومات، عصر التحول إلى الاقتصاد الرقمي القائم على المعرفة، الذي أمست فيه المعلومات المحدد

الاستراتيجي لرأس المال ونمت فيه مكانة رأس المال الفكري في مقابل رأس مال الموجودات، وتحولت فيه السلوكيات والعلاقات واستراتيجيات الأداء والإدارة والإنتاج وتقديم الخدمة إلى مزيد من الاعتماد على نظم الكمبيوتر وشبكات المعلومات (وفي مقدمتها الإنترنت) ؟

لقد برزت تحديات قانونية كثيرة لتقنية المعلومات على النظم القانونية، ابتدأت منذ مطلع السبعينات ومرت عبر مسيرة متسارعة الأحداث، خلفت وراءها مسائل قانونية أوجبت ظهور سلسلة من موجات التشريع في حقول قانونية مختلفة :- (الخصوصية وحماية البيانات الشخصية وبنوك المعلومات (حقوق إنسان - تنظيم إداري)، جرائم الكمبيوتر والشبكات (قانون جنائي موضوعي)، الملكية الفكرية للمصنفات الرقمية (قانون مدني بالنسبة للحق المعنوي وقانون الملكية الفكرية كفرع خاص)، القواعد الإجرائية الجزائية لمواجهة جرائم التقنية العالية (أصول إجرائية جنائية)، تشريعات الأمن والمعايير والمقاييس التقنية (تشريعات تنظيمية وإدارية وتتصل بحماية المستهلك وتتصل أيضا بتشريعات الاتصالات والمعلومات) تشريعات الإثبات بالوسائل الالكترونية وحجية مستخرجات الحاسوب (قانون البيانات)، تشريعات المحتوى الضار وغير المشروع لمواقع المعلوماتية - (النشر الإلكتروني والمطبوعات والصحافة وقواعد السلوك والإعلان وتتصل بعضها بحماية المستهلك)، تشريعات الوسائل المؤتمنة في الحقل المالي والبنوك الالكترونية (مال وأسواق مالية ومصارف)، تشريعات حماية المستهلك في عصر المعلومات، وتشريعات التجارة الإلكترونية والتوقيعات الرقمية (تجاري وتعاقد واثبات وضرائب وإداري - أي إدارة حكومية بالنسبة للخدمات والمشتريات الحكومية ضمن مفهوم الحكومة الإلكترونية)، وقد أوجبت هذه الحقول اتخاذ تدابير تشريعية أما بوضع تشريعات خاصة في هذه الحقول كل على حدة، أو ضم أكثر من حقل في تشريع مستقل واحد أو من خلال إجراء تعديلات امتدت للعديد من التشريعات المدنية والتجارية والجزائية والإدارية في العديد من دول العالم الصناعية، ومن هنا مثلا، نجد هذه الدول تتبنى استراتيجية الحد الأدنى من التنظيم القانوني للتجارة الإلكترونية التي تعتمد على التنظيم القانوني للمسائل المتقدمة، وهو أمر طبيعي بالنسبة لها - وليس لنا - لان هذه الدول تواءمت مع هذه المسائل ووضعت تشريعات عديدة في هذه الحقول، أما في البيئة العربية، فان مجتمعاتنا لم تتقاطع مع هذه الموجات التشريعية - إلا في حدود بعض المسائل الرئيسة في حقل الملكية الفكرية للمصنفات الرقمية كبرامج الحاسوب وقواعد البيانات والدوائر المتكاملة بسبب التزامات دولنا للدخول في عضوية منظمة التجارة الدولية وبسبب متطلبات اتفاقية ترانس الخاصة بالملكية الفكرية إضافة إلى بعض المسائل المتعلقة بالمقاييس والمواصفات وتشجيع الاستثمار والجمارك والاتصالات في المسائل المرتبطة بالتقنية، وجهد نام يتواصل هذه الأيام بشأن التجارة الإلكترونية على ما أوضحنا فارطاً، أما فيما عدا ذلك، فلم يتحقق شيء يذكر رغم إن الدول العربية تبنت منذ نهاية العام المنصرم مبادرات متقدمة في حقل تقنية المعلومات كما بالنسبة لمشروعات مدينة دبي للانترنت وسوق دبي الالكترونية في دولة الإمارات العربية، ومبادرات القرى الذكية في مصر، ومبادرة تقنية المعلومات في الأردن وما تبعها من تبني مفهوم

وشعار الحكومات الالكترونية في كل من دبي والأردن ومصر وقطر والبحرين وغيرها.<sup>23</sup> ويمكننا في ضوء قراءة التجربة العربية في التعامل مع العصر الرقمي واحتياجاته التشريعية، أن نلاحظ تخبطا في التعامل مع المتطلبات التشريعية لتقنية المعلومات، وهو أشبه بحالة التخبط التي شهدتها النظم المقارنة في مطلع السبعينات وخلال الثمانينات، ولا تزال تشهد بعضا من ملامحه في عدد من مسائل تقنية المعلومات في الوقت الحاضر، ففي هذا السياق، يلمس المتابع عدم وضوح الرؤية، ويلمس اتجاه المؤسسات التشريعية في الدول النامية - ومنها العربية - إلى حلول مبتسرة وليست حلولا كافية تدرك التحديات التقنية ذاتها وتدرك حالة التغير والتطور في الاحتياجات القانونية لمواجهة العصر الرقمي، وتدرك أكثر أن الحلول المقتبسة دون إعادة توافر وعي ومدروس على الأقل، حلول معطلة وليست فاعلة لاعتبارات اجتماعية وسياسية واقتصادية وقانونية، حتى أننا لا نكون مبالغين إن قلنا أن هذه الحلول الجزئية المقتبسة تزيد التحديات ولا توفر حلولاً لها، كما أنها في بعض الأحيان تقيم مزيداً من العوائق نحو الأهداف النبيلة في خطط توظيف التقنية بدلا من أن تذلل هذه العوائق.

إن شيوع الكمبيوتر وفيما بعد الاتجاه نحو التشبيك عبر مختلف أنواع شبكات المعلومات وفي مقدمتها الانترنت وبناء شبكات وقواعد المعلومات، افرز حاجة ملحة للتدخل من اجل حماية امن المعلومات وحماية الخصوصية والتنظيم الصحيح لحماية الملكية الفكرية ومراعاة أثارها على المجتمع، ومن اجل حماية المستهلك والاعتراف بالحجج وملائمة الوسائل الإلكترونية للتصرفات القانونية بنفس القدر من الملائمة المقبولة والمعترف بها للوسائل غير الإلكترونية، إلى جانب أهمية تنظيم معايير ومقاييس التقنية وحماية المستخدم في نطاقها وتنظيم البنى التحتية ضمن تدابير تكفل نماء توظيف التقنية بشكل صحيح وملائم لحاجات المجتمع.<sup>24</sup>

إن اخطر ما يواجه فعالية نظم حماية المعلومات وفعالية الأدوات التشريعية لتنظيم استخداماتها وتطبيقاتها وصورها المعالجات الجزئية للتحديات القانونية المتصلة بتقنية المعلومات، تلك المعالجات التي يظن البعض أنها الحل القانوني الكامل، في حين أنها قطعة سيفسائية من لوحة قانون تقنية المعلومات، والأخطر أنها حلول لم تدرك عاملين رئيسيين، الأول: أننا نتحدث عن تنظيم مسائل أثرت منذ منتصف الستينات تقريبا، ودراسة مسيرتها التاريخية يدلنا على اتجاهات تطورها مستقبلا، فان لم يدرك الماضي ولم يستشرف المستقبل أصبحنا كأننا ننظم الحاضر فقط، فان أضفنا انه حاضر غيرنا لا حاضرا أصبحت المخاطر أكثر عمقا وأكثر احتمالية للتحقق وأصبح التدبير غير ذي اثر. والثاني: إنها مسائل تعرضت للتشويه أو على الأقل غياب المقاييس العلمية لتبيان الصواب والخطأ بشأنها، وكبديل على إعادة التقييم الواعي من قبل الجهات المتخصصة في هذا الحقل، اعتمدنا فكرة الثقة بتقدير جهات خارجية اقل ما توصف أنها ذاتها لا تزال تعاني تحديات الصواب والخطأ وتجرب وتعيد التجربة، مما يعني أن ما نثق به محل شك، ولهذا يصبح التدبير ذاته محل شك.

وفي الأخير لن يكون كافيا القول في نظام قانوني ما أن قانون التواقيع الرقمية مثلا قد حل مشكلة التجارة الالكترونية أو حل مشكلات وتحديات الحكومة الالكترونية أو الأعمال

المصرفية الالكترونية، أو انه فعلا سيحل مشكلة الأعمال اللاسلكية الخلوية الأخذة في النماء على نحو افرز مفهوما جديدا لتبادل المعطيات وأداء الخدمات عن بعد، فتنظيم حجية المعاملات الالكترونية مثلا مجرد جزئية في فضاء تملؤه التحديات، تلك التحديات التي تمتد إلى مسائل التنظيم القانوني لأمن المعلومات التي تنتهي بدورها إلى تجربة تاريخية وتشريعية لها مزاياها ومتطلباتها، وتمتد لمسائل الخصوصية التي أصبحت تنظم ضمن أدوات تتعدد طبيعتها تمتاز بالشمولية وكثرة المسائل محل التنظيم التي تفوق تدييرا تشريعا جزئيا، وكذلك مسائل الملكية الفكرية للعناصر الرقمية ومسائل التقاضي وإجراءاته في هذه البيئة وغيرها الكثير من التحديات.

### الخاتمة:

إن المعلوماتية أو المعلومات واستخدماتها المختلفة أدت إلى ظهور مشاكل جديدة وعراقيل كبيرة، في نطاق القانون الجنائي الدولي، وفي غيره من فروع القانون، ذلك أن الإجرام المعلوماتي له طبيعة خاصة متميزة وذلك لعدة اعتبارات من بينها: طبيعة المال المعلوماتي وحدثة الحاسوب وتقنية تشغيله وحدثة ظاهرة المجرم المعلوماتي ذو المهارات التقنية العالية، وبالتالي من الواضح أن هناك نقصا تشريعا في مجال الجرائم المعلوماتية بالنسبة للتشريع المغربي، ولذلك وجب على المشرع أن يتدخل ليشمل بالحماية كل الأموال المعلوماتية وكل الأشخاص بمعناهم الواسع في ظل النصوص التقليدية الحالية والتي أصبحت غير ملائمة للتطبيق في مجال الجريمة المعلوماتية.

### الهوامش:

- 1 عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دار، مديولي، القاهرة، 2009، ص115.
- 2 عمر الفاروق الحسيني، تأملات في بعض صور الحماية الجنائية لبرامج الحاسب الآلي، مجلة المحاماة، عدد نوفمبر/ديسمبر 1989، القاهرة، ص 13.
- 3 زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 أكتوبر، 1993، ص ص 471 و472.
- 4 نفس المرجع، ص472
- 5 مفتاح بوبكر المطردي، الجريمة الالكترونية والتغلب على تحدياتها، في المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25 / 9 / 2012، ص12.
- 6 سالم محمد الأوجلي، التحقيق في جرائم الكمبيوتر و الإنترنت، تاريخ الولوج: 2018/03/02، على 15.30، لمعلومات أوفر أنظر: [/http://afaitouri.maktoobblog.com/1624946](http://afaitouri.maktoobblog.com/1624946)
- 7 محمد علي العريان. الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، القاهرة، 2004، ص: 48.
- 8 نفس المرجع، ص48.
- 9 ممدوح خليل عمر، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة، 1983، ص 207
- 10 أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994، ص 48
- 11 بدر سليمان لويس، أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية رسالة دكتوراه في حقوق، جامعة القاهرة، 1982، ص148
- 12 عبد الفتاح بيومي حجازي، المرجع السابق، ص 620
- 13 David Bainbridge, Introduction to computer law, third edition, Pit Man publishing, 1996, p237
- 14 محمد إبراهيم محمد الشافعي، النقود الإلكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع 1، يناير، 2004، ص ص 142-148.

- 15 محمد علي العريان، مرجع سابق ، ص46.
- 16 نفس المرجع، ص47
- 17 منير محمد الجنبهي، وممدوح محمد الجنبهي، جرائم الانترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعية. طبعة 2004. ص 96.
- 18 نفس المرجع، ص96
- 19 نفس المرجع، ص101
- 20 فاروق علي الحفناوي، قانون البرمجيات القانونية لبرمجيات الكومبيوتر. دارالكتاب الحديث. القاهرة، 2000، ص ص 112-113.
- 21 نفس المرجع، ص115
- 22 محمد أحمد أمين الشوابكة، الجريمة المعلوماتية، دارالثقافة، عمان. 2004، ص120
- 23 يونس عرب، تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، ورقة عمل " الاتجاهات التشريعية للجرائم الالكترونية، هيئة تنظيم الاتصالات / مسقط – سلطنة عمان 2-4 ابريل 2006، صص 29-30
- 24 نفس المرجع، ص31