جامعة عباس لغرور خنشلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

نيابة العمادة لما بعد التدرج
والبحث العلمي والعلاقات الخارجية

السياسة الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

أطروحة مقدمة لنيل شهادة دكتوراه ل.م.د في الحقوق
تخصص: قانون دولي جنائي

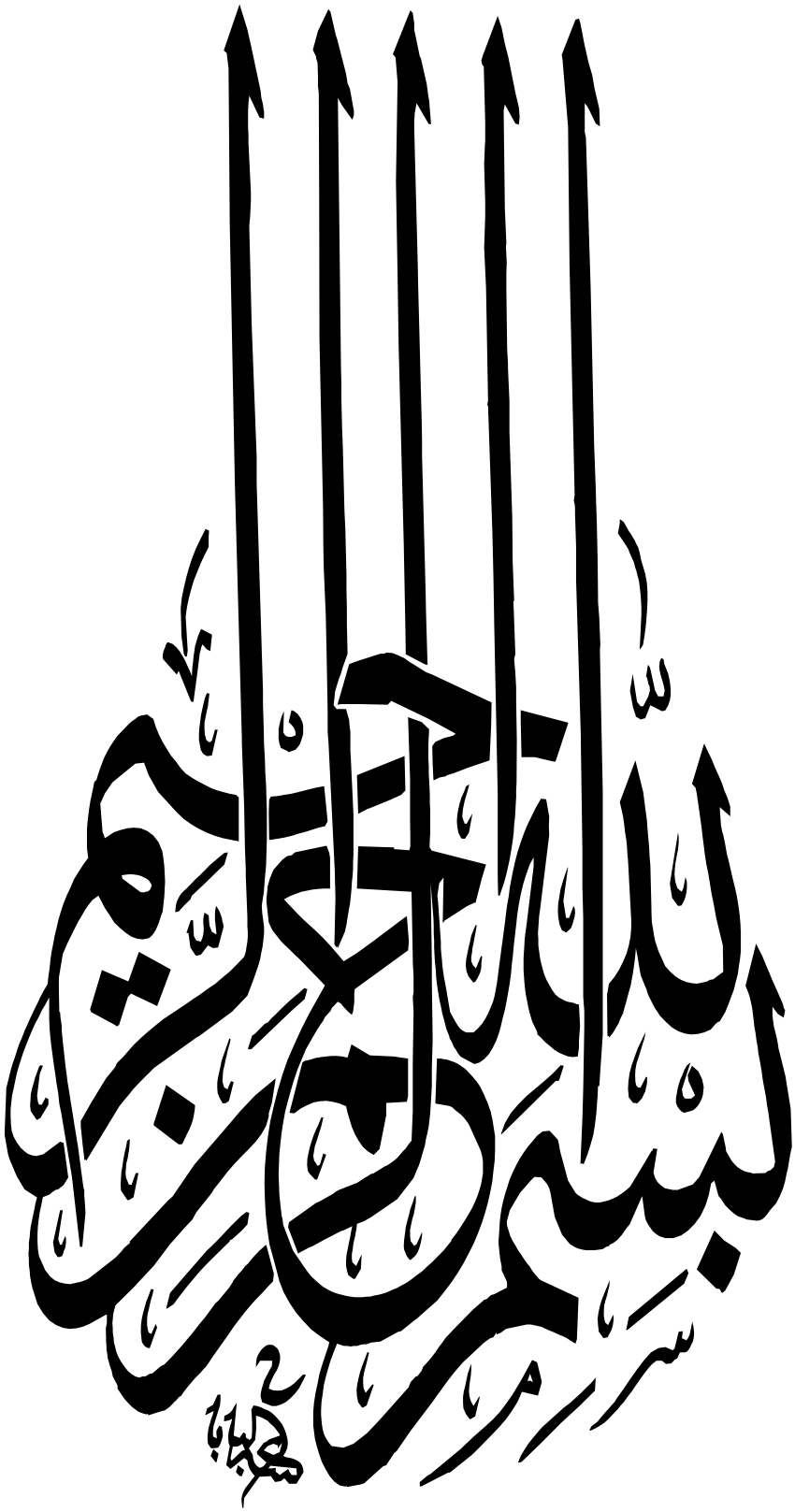
إعداد الطالبة:
زراري نسرين

إشراف الأستاذ الدكتور:
بوقرة اسماعيل

لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الجامعة الاصلية	الصفة
بن مكي نجاة	أستاذ	جامعة خنشلة	رئيسا
بوقرة إسماعيل	أستاذ	جامعة خنشلة	مشرفا ومقررا
زمورة داود	أستاذ محاضر أ	جامعة خنشلة	عضوا ممتحنا
زبيري مارية	أستاذ محاضرأ	جامعة خنشلة	عضوا ممتحنا
بوكماش محمد	أستاذ	جامعة باتنة 01	عضوا ممتحنا
بوترعة سهيلة	أستاذ محاضر أ	جامعة البويرة	عضوا ممتحنا

السنة الجامعية: 2024/2023


بسم الله الرحمن الرحيم

شكـــر وتقـديـــر

أشكر " الله عز وجل" بداية الذي وفقني لإنجاز وإتمام هذا العمل

أتقدم بخالص شكري وتقديري:

إلى أستاذي الفاضل " البروفيسور بوقرة اسماعيل"

تقديرا لمجهوداته وتوجيهاته السديدة وعرفانا بفضله لما قدمه لي من نصائح وتوجيهات وملاحظات

كما أتقدم بجزيل الشكر إلى هيئة اللجنة الموقرة التي قبلت مناقشة هذا العمل

كما أشكر جميع أساتذتي في مختلف أطوار ومراحل دراستي، وكل أسرة كلية الحقوق والعلوم السياسية

بجامعة عباس لغرور – خنشلة

وكل من قدم لي يد المساعدة من قريب أو من بعيد

الإهـــــداء

أهدي ثمرة جهدي

إلى من ساند خُطاي، ومهد لي طريق العلم وشجعني ودعمني من أجل أن أعتلي سلم النجاح أبي حفظه الله وشفاه.

قائمة المختصرات

- **د.ب.ن:** دون بلد النشر
- **د.د.ن:** دون دار النشر
- **د.س.ن:** دون سنة النشر
- **ج.ر.ج.ج:** الجريدة الرسمية للجمهورية الجزائرية
- **دج:** دينار جزائري
- **د.ط:** دون طبعة
- **ص:** الصفحة
- **ط:** الطبعة
- **ق.إ.ج.ج** : قانون الإجراءات الجزائية الجزائري
- **ق.ع.ج:** قانون العقوبات الجزائري
- **ق.ع.ف:** قانون العقوبات الفرنسي
- **م:** المادة

TABLE D'ABRÉVIATIONS :

Adresse IP: Internet Protocol

Art: article

GDPR: General Data Protection Regulation

Ibid: Référence identique à la précédente

N° : Numéro

Op.Cit: opus citatum (précité) / Ouvrage précédemment cité

P: page

Para : Paragraph

T: Tome

Vol: Volume

مقدمة

مقدمة:

ظهر حديثا نوع جديد من الأمن يتمثل في الأمن المعلوماتي الذي أصبح يطلق عليه حاليا تسمية الأمن السيبراني، وهو أمن أنظمة المعالجة الآلية للمعطيات، والمعطيات الرقمية، والشبكات.

هذا الأمن يواجه العديد من التحديات أهمها التهديدات السيبرانية التي تتخذ قالبا معينًا، والمتمثلة تحديدًا في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وهي مختلف الجرائم التي يكون هدفها نظام المعالجة الآلية للمعطيات في حد ذاته، أو معطياته بمختلف أنواعها، أو تلك التي يسُتخدم فيها هذا النظام كوسيلة لارتكابها لاسيما إذا كان مرتبط بشبكة الانترنت.

فالجرائم التي تُستخدم فيها أنظمة المعالجة الآلية للمعطيات كوسيلة أصبحت في عالم موازي لعالم الإجرام التقليدي، حيث تكنولوجيات الإعلام والإتصال أضفت على غالبية الجرائم التقليدية حُلة جديدة وأصبحت أنظمة المعالجة الآلية للمعطيات وسيلة لإرتكابها، فأصبحت كل جريمة تقليدية متعارف عليها هناك جريمة سيبرانية تقابلها، وهذا بسبب سوء إستخدام الانترنت وتكنولوجيات الاعلام والاتصال، لذا كان لابد من التوجه نحو حوكمة الأنترنت.

والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تعتبر من الجرائم المستحدثة التي تزداد كل يوم وتتزايد مخاطرها وأضرارها فلم تصبح مخاطرها تهدد الأشخاص الطبيعية فقط بل أصبحت في الغالب تهدد الأشخاص المعنوية والحكومات والدول، خاصة في ظل التوجه نحو الإدارة الإلكترونية وتجسيد الحكومة الإلكترونية في غالبية الدول.

فالتطور التكنولوجي يعتبر دائما سباق على التشريعات الوضعية بمختلف أنواعها، وهذه التشريعات تسعى دائما للتماشي مع التطورات التكنولوجية، ومسايرتها بغرض توفير حماية قانونية من الإعتداءات الناجمة عنها والماسة بالأشخاص وأموالهم وتنظيمها قانونيا وفقا لقالب موضوعي وإجرائي يضمن عدم المساس بالحقوق الأساسية والموازنة بين حقوق

الضحايا وحقوق مرتكبي هذه الجرائم، هذا ما يفرض تبني سياسة جنائية حديثة لمكافحة هذه النوع من الجرائم المستحدثة والمتمثل كما سبق وعرجنا في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي تتميز بنوع من الخصوصية يختلف عن السياسة الجنائية المتبناة لمكافحة الجرائم التقليدية.

لذا فنجد على المستوى الدولي تم تجسيد سياسة جنائية لمكافحة هذا النوع من الجرائم، تقوم على التعاون الدولي وتكاثف الجهود الدولية لمواجهة هذا الإجرام المستحدث العابر للحدود الوطني في غالب الأحيان، وتأثرًا بما هو موجود في المحيط الخارجي وبما هو موجود داخليا وبسبب ظهور العديد من الجرائم والاعتداءات السيبرانية على المستوى الوطني في الجزائر، وتفاقمها وبغرض تفادي القصور التشريعي في الجانبين الموضوعي والإجرائي، ومواءمة للتشريعات الدولية على المستوى العالمي والإقليمي، تم إستحداث قواعد جنائية موضوعية، وقواعد جنائية إجرائية على ضوء السياسة الجنائية المعاصرة تتماشى والطبيعة الخاصة لهذه الجرائم.

وللجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات مسميات عديدة منها الجرائم المعلوماتية، أو الجرائم الالكترونية، أو الجرائم السيبرانية، والتسمية التي اعتمدناه في هذه الدراسة هي الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات كونها تركز على الاعتداء على أنظمة المعالجة الآلية للمعطيات، واستخدام هذه الأخيرة في إرتكاب الجرائم، ولا تركز على المعطيات فقط.

فهذه الدراسة تنصب على الجرائم التي تستهدف نظام المعالجة الآلية للمعطيات حيث تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات المنصوص عليها بموجب قانون العقوبات الجزائري، ومختلف الجرائم التي ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية.

ونظام المعالجة الآلية للمعطيات عرفته اتفاقية بودابست في مادتها الأولى بأنه «يقصد ب "منظومة الكومبيوتر" أي جهاز أو مجموعة من الأجهزة المتصلة أو المتعلقة ببعضها

البعض، ويقوم واحد منها أو أكثر، تبعا لبرنامج، بعمل معالجة آلية للبيانات[1]»، وعرفته الاتفاقية العربية كذلك في مادتها الثانية بأنه" مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات"[2]، وعرفه المشرع الجزائري في المادة 2 من القانون 09-04 بأنه منظومة معلوماتية ويتمثل في "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[3].

يتكون هذا النظام من مجموعة من العناصر المادية والعناصر المنطقية، فمن خلال هذه الدراسة تطرقنا إلى الجرائم التي تستهدف النظام في حد ذاته والمتمثلة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ويعتبر أهم نموذج لها جريمة الدخول والبقاء عن طريق الغش للنظام، والتي تترتب عليها عدة جرائم أخرى وتتمثل أهمها في الجرائم الماسة بالمعطيات في حد ذاتها والتي ركزنا عليها من خلال دراستنا حيث تطرقنا إلى الجرائم الماسة بالمعطيات بمختلف أنواعها، ويمكن أن تكون هذه الجرائم مستقلة عن جريمتي الدخول والبقاء غير المشروع، وتطرقنا كذلك إلى الجرائم الماسة بنوع محدد من المعطيات وهي جرائم المساس بالمعطيات الشخصية.

إضافة إلى الجرائم التي يسهل نظام المعالجة الآلية للمعطيات إرتكابها أو التي ترتكب بواسطته، رغم أنه في الأونة الأخيرة غالبية الدراسات عكفت على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات باعتبارها تمثل الجريمة المعلوماتية البحتة، مع إهمالها للجرائم التقليدية المرتكبة بواسطة النظام أو التي يسهل هذا الأخير إرتكابها رغم خطورتها كذلك، إضافة إلى جرائم مواقع التواصل الإجتماعي التي استفحلت في الأونة الأخيرة.

---

[1] المادة 1 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية، الموقعة في 23 نوفمبر 2001 بعاصمة المجر بودابست.

[2] المادة 2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية العربية.

[3] المادة 2 من القانون 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47، المؤرخة في 25 شعبان عام 1430، الموافق ل16 غشت سنة 2009.

أهمية الدراسة:

تتجلى أهمية دراسة موضوع "السياسة الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات" فيما يلي:

الأهمية العملية:

_ تماشي السياسة الجنائية مع التطورات والمستجدات الحاصلة للجريمة التي بدورها أصبحت تتخذ أشكالا جديدة تتمثل في الجرائم المستحدثة التي محلها البيئة السيبرانية والمعطيات الرقمية.

_ ضرورة تطويق الجرائم المتعلقة بأنظمة المعالجة الآلية بمختلف أنواعها، كون الإعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات أو التي تكون بإستخدامها، آثارها تمتد من المستوى الوطني إلى المستوى الدولي وتمس الأشخاص والحكومات والأموال على حد سواء.

_ دراسة السياسية الجنائية الدولية والوطنية المتبعة لمواجهة هذه الجريمة من خلال التطرق إلى مواطن قوتها وضعفها، والتحديات التي تواجهها في مجابهة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بغرض تقييمها، وإبراز النقص والفراغ التشريعي إن وجد في هذا الشأن لأجل التوصل إلى حلول تشريعية على المستوى الدولي والوطني لمجابتها، دون الحيدة عن السياسة الجنائية المعاصر.

الأهمية العلمية:

باعتبار موضوع الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من أهم المواضيع القانونية المستجدة في التشريع الجزائري، فنظامها القانوني يكتنفه نوع من الغموض، لذا لم تتم دراسته بعد بشكل شاملا، حيث أن أغلب العناصر الرئيسية في هذا الموضوع، لاتزال تحتاج بحث ودراسة، ولأنه يعتبر من المواضيع الدقيقة التي يجب على الباحث القانوني فيها أن يكون ملم بشق قانوني من الناحية الموضوعية والاجرائية إضافة إلى درايته بالشق التقني

والفني، لذا من خلال هذه الدراسة سنسلط الضوء على هذا الموضوع بشكل مفصل، بغرض الإسهام في إثراء الدراسات القانونية.

أسباب اختيار الموضوع:

الأسباب الذاتية لاختيارنا لهذا الموضوع هو تطلعي للبحث في الجرائم المستحدثة التي أصبحت محل اهتمام على المستوى الوطني والدولي، والتي تعتبر الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ابرز نمط لها.

الأسباب الموضوعية لاختيارنا لهذا الموضوع كون موضوع البحث يتعلق بجرائم أصبحت تشكل تهديدا كبيرا على الأشخاص والأموال والحكومات، ونظرا لأنه ينصب على إبرازالسياسة الجنائية المتبعة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بغرض تطويقها والتقليل منها ولما لا الحد منها.

أهداف الدراسة:

تهدف هذه الدراسة إلى الوقوف على السياسة الجنائية التي انتُهجت لأجل التصدي إلى الجرائم المتعلقة بأنظمة معالجة المعطيات و مكافحتها سواء على المستوى الدولي أو المحلي، من خلال التطرق إلى مختلف الآليات الدولية سواء من الناحية الموضوعية أو الإجرائية، ودراسة كذلك الآليات الموضوعية والإجرائية التي اعتمدتها الدولة الجزائرية على مستواها الداخلي وتقييمها، ومعرفة الحلول التشريعية الوطنية المستحدثة التي فرضها هذا النوع من الإجرام والتي هي انعكاس لطبيعته و خصوصيته المتطورة بصفة مستمرة.

على هذا الأساس ينبغي تبيان مدى نجاعة السياسية الجنائية المنتهجة على الصعيدين الدولي والوطني لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

واستنادا لذلك نطرح الاشكالية التالية: **مامدى كفاية التشريعات الدولية والتشريع الوطني في بلورة السياسة الجنائية المنتهجة على المستوى الدولي والوطني لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات؟**

وانطلاقا من هذه الإشكالية تُطرح التساؤلات التالية: فيما تتمثل الآليات التشريعية على المستوى الدولي وعلى المستوى الوطني لتصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات؟ وما مدى كفايتها وفعاليتها في مكافحة هذه الجرائم المستحدثة؟ وهل ساير المشرع الجزائري مقتضيات الإتفاقيات الدولية في هذا الشأن؟

منهج الدراسة:

وإجابة منا على الإشكالية الرئيسية المطروحة، وعلى التساؤولات المتفرعة عنها وتماشيا مع طبيعة الدراسة التي تحدد المنهج المتبع، والأدوات المعتمدة فيها، فإنه تم الاعتماد في

هذه الدراسة على منهجيين رئيسسن وهما:

المنهج الوصفي: جمع مختلف النصوص القانونية الدولية والوطنية التي وردت في سياق الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

المنهج التحليلي: من خلال تحليل مختلف النصوص القانونية الدولية والوطنية والتعليق عليها، وتقييم فعاليتها في مكافحة هذه الجرائم.

إضافة إلى ذلك اعتمدنا على **المنهج المقارن بصفة غير أساسية**، من خلال اعتماد أدواته للمقارنة بين النصوص القانونية حينما يتطلب الأمر ذلك.

الدراسات السابقة: وجدنا دراسات سابقة باللغتين العربية والفرنسية

الدراسات السابقة باللغة العربية:

أطروحات الدكتوراه:

– بوحليط يزيد، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة دكتوراه، كلية الحقوق، قسم القانون الخاص، جامعة باجي مختار عنابة، 2016.

تطرق الباحث في أطروحته إلى الأحكام الموضوعية في مكافحة الجرائم الإلكترونية في الباب الأول، وإلى الأحكام الإجرائية في مكافحة الجرائم الإلكترونية في الباب الثاني، وأهم

أوجه الإختلاف بين هذه الدراسة ودراستنا، هي أن دراستنا تختلف عن هذه الدراسة من حيث النطاق كونها إشتملت على الأحكام الموضوعية والإجرائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الدولي والتي لها أهمية بالغة كونها تؤثر على السياسة الجنائية الوطنية المتبعة لمكافحتها وعلى تشريعاتها الداخلية الموضوعية والإجرائية، إضافة إلى إشتمالها على الأحكام الموضوعية والإجرائية على المستوى الوطني، إضافة إلى ذلك أن دراستنا هذه تطرقنا فيها للجرائم الماسة بالمعطيات الشخصية باعتبارها من أهم الجرائم السيبرانية المستحدثة لمساسها بمعطيات نظام المعالجة الآلية للمعطيات، ولارتباطها بأهم حق مكرس إتفاقيا ودستوريا وهو الحق في الحياة الخاصة، إضافة إلى تطرقنا إلى الأقطاب الجزائية والقطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. وعليه هذا الإختلاف يجعل دراستنا أوسع وأشمل من حيث العناصر التي تمت دراستها، ما يضفي على دراستنا طابع الشمولية والدقة في الطرح والمعالجة.

-عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الجنائي، جامعة تبسة، 2018/2017.

تطرقت الباحثة في هذه الأطروحة إلى "الحماية الجنائية للمعطيات الرقمية"، وذلك من خلال بابين، الأول موسوم بالأحكام الموضوعية للحماية الجنائية للمعطيات الرقمية، والثاني موسوم بالأحكام الإجرائية للحماية الجنائية للمعطيات الرقمية. وهذه الدراسة تختلف عن دراستنا من حيث النطاق حيث أن الباحثة اقتصرت دراستها على الحماية الجنائية للمعطيات الرقمية والتي يمثل الإعتداء عليها إحدى جرائم المساس بأنظمة المعالجة الآلية للمعطيات وهي جريمة الإعتداء على المعطيات، بينما نطاق دراساتنا أوسع فهي تنصب على جميع جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وتختلف عن دراستنا كذلك في أنها لم تتطرق إلى الحماية الجنائية المكرسة للمعطيات وفقا للقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. إضافة إلى آليات الحماية الجنائية الموضوعية والإجرائية على المستوى الدولي للمعطيات الرقمية بصفة عامة

والشخصية بصفة خاصة، هذا ما يجعل دراستنا تتطرق إلى الحماية الجنائية للمعطيات الرقمية بكل أنواعها على المستويين الدولي والوطني خلافا لسابقتها، وذلك حتى نتوصول إلى تأثير السياسة الجنائية الدولية على الوطنية في هذا الشأن، بغية تقديم إقتراحات تعزز حماية هذه المعطيات وخاصة الفئة الحساسة منها.

الكتب:

_ بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، د.ط، دار الخلدونية، الجزائر، 2017.

قسمت الدكتورة كتابها إلى ثلاثة فصول كالتالي: الفصل الأول ماهية الجرائم المعلوماتية، الفصل الثاني الآليات الدولية لمكافحة الجرائم المعلوماتية، الفصل الثالث الآليات الوطنية لمكافحة الجرائم المعلوماتية، وهذه الدراسة تعتبر أقرب دراسة لموضوعنا، حيث تتفق مع دراستنا في نطاق الدراسة على المستويين الدولي والوطني، إلا أن أوجه الاختلاف تكمن في أن دراستنا أضافت الجهود الدولية والتشريعات الدولية المتعلقة بالمعطيات الشخصية، والقواعد القانونية لحماية المعطيات الشخصية الموضوعية والإجرائية، وبعض القواعد الإجرائية المستحدثة في قانون الإجراءات الجزائية، والأحكام المتعلقة بالقطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. ما يجعل دراستنا شاملة ومحينة تتماشى مع المستجدات الدولية والتشريع الوطني الساري المفعول.

الدراسات السابقة باللغة الفرنسية:

Romain BOOS, La lutte Contre La cybercriminalité Au Regard De L'action Des états, Doctorat De Droit privé Et sciences Criminelles, Université De Lorraine, 2016.

تطرق الباحث في هذه الأطروحة إلى مكافحة الجريمة السيبرانية على ضوء الإجراءات التي اتخذتها الدول، حيث تم تقسيمها إلى جزئيين رئيسيين، الأول تطرق فيه الباحث إلى عدم ملائمة النظام القضائي لجرائم الفضاء السيبراني، أما الثاني تطرق فيه إلى صعوبات التعاون

الدولي. فهي تختلف عن دراستنا من حيث نطاق الدراسة لأنها اقتصرت على الجانب الإجرائي على المستوى الدولي وعلى المستوى الاقليمي الأوربي.

صعوبات الدراسة:

ومن الصعوبات التي واجهتنا في هذه الدراسة، قلة المراجع المتخصصة والدقيقة في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، هذا من جهة ومن جهة أخرى تقريبا شبه إنعدام للأحكام القضائية والقررات التي تبرز موقف القضاء الجزائري من هذه الجرائم، ويقابلها غياب تام للإجتهادات القضائية.

نقص الإحصائيات الدقيقة من الجهات الرسمية، وانعدامها أحيانا، وحتى إن وجدت فإنها لا تعبر عن حقيقة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات المرتكبة فعلا، وهذا مرده أمرين أساسيين كونها تعتبر من أكثر الجرائم الخفية الغير ظاهرة للعيان كونها تُرتكب في بيئة سيرانية غير مادية، وثانيهما كونها تعتبر من الجرائم المسكوت عنها التي تقل فيها نسبة التبليغ بشكل كبير وهذا راجع إلى طبيعة الجريمة في حد ذاتها وصعوبة كشفها وصعوبة علم الضحية في الغالب بوقوعها لاسيما وإن كان شخص طبيعي، وإن علموا فإنهم كثرا ما يحجمون عن التبليغ لخوفهم من المساس بشرفهم وسمعتهم وإن كانوا أشخاص معنويين خوفهم من خسارة عملائهم وفقدان الثقة بهم كون أنظمتهم غير آمنة، وهذا يشكل عائق كبير أمام تقييم الآليات القانونية المتبعة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الوطني تقيما موضوعيا.

إضافة إلى التعديلات المتتالية على قانون العقوبات وقانون الإجراءات الجزائية، التي تتطلب تحيين الدراسة وفقا للمستجدات التشريعية الوطنية.

وتبعًا لما سبق التعريج عليه قسمنا موضوع "السياسية الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات" تقسيما ثنائيا إلى بابيين، وكل باب إلى فصلين وفقا للخطة التالية:

الباب الأول: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الفصل الأول: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الموضوعي

الفصل الثاني: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الإجرائي

الباب الثاني: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الفصل الأول: السياسة الجنائية الوطنية لمكافحة جرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الموضوعي

الفصل الثاني: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الإجرائي

وتم اختتام دراسة هذا الموضوع بسرد مجمل النتائج التي توصلنا إليها، واقتراح جملة من الاقترحات التي ارتأينا أنها تساهم في تعزيز هذه الدراسة.

الباب الأول: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الباب الأول: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

أصبحت التهديدات السيبرانية المُجَرّمَة التي محلها الفضاء السيبراني، تُشكل مساس كبيرًا بالدول والمؤسسات والأشخاص، فلم تعد القوانين الداخلية لها إمكانية التصدي لها ومكافحتها، وذلك اعتبارًا لخصوصيتها المميزة التي تختلف عن بقية الجرائم التقليدية المعروفة، كونها جرائم ناعمة عابرة للحدود الوطنية متطورة بشكل مستمر من ناحية أشكالها وأساليب وتقنيات إرتكابها، ما استدعى بالضرورة تكاثف الجهود الدولية بين الدول لوضع سياسة جنائية دولية لمكافحتها والتصدي لها على كل من المستوى العالمي والإقليمي، بإيجاد آليات تعاون دولي من الناحية الموضوعية وكذلك الإجرائية.

وهذا بهدف تبني سياسة جنائية دولية موحدة قائمة على التعاون الدولي على المستويين العالمي والإقليمي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال اعتماد الدول على الاتفاقيات الدولية الخاصة بهذا الشأن، وتنسيق التعاون وتبادل الجهود بين الدول.

ارتأينا تقسيم هذا الباب إلى فصلين السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الموضوعي (كفصل أول) ثم إلى السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الإجرائي(كفصل ثاني).

الفصل الأول: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الموضوعي

نظرا لخطورة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، برزت الكثير من الجهود الدولية لغرض إيجاد حلول لمكافحتها والتقليل منها، والإعراب عن خطورتها على الدول وأمنها، فتم عقد العديد من المؤتمرات الدولية في هذا الشأن، التي انبثقت منها عدة توصيات، وأُصدِرت الكثير من القرارات والتوجيهات.

ونتيجة لهذه الجهود الدولية كرست المنظمات الدولية عدة آليات قانونية إتفاقية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وأبرزها الإتفاقيات الدولية المتبناة على الصعيدين الإقليمي والعالمي التي تُرتب على الدول إلتزامات بمجرد المصادقة عليها، ما يجعلها فعالة في التصدي لهذه الجرائم.

لذا قسمنا هذا الفصل إلى مبحثين، جهود المنظمات الدولية في بلورة التشريعات الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الأول)، التشريعات الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الثاني).

المبحث الأول: جهود المنظمات الدولية في بلورة تشريعات دولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يمكن أن تتخذ شكل الجريمة المنظمة عبر الوطنية[1]، التي تتطلب تكاثف الجهود لمكافحتها، لذلك برزت العديد من الجهود الدولية بغرض التصدي لها والتقليل من مخاطرها ولما لا السعي الحد منها فتجلت جهود المنظمات الدولية على المستوى العالمي والإقليمي، وتجلى دورها في رصد السياسة الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، كونها تعتبر من أهم المؤسسات الفاعلة في المجتمع الدولي.

قسمنا هذا المبحث إلى مطلبين: دور المنظمات الدولية العالمية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، دور المنظمات الدولية الاقليمية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الثاني).

[1] الجريمة المنظمة عرفتها المادة 02 من إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة بموجي قرار رقم 25/55 بتاريخ 15 نوفمبر سنة 2000، المصادق عليها بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فيفري 2002، ج.ر.ج.ج، عدد 09، صادر بتاريخ 10 فيفري 2002.

" يقصد بتعبير جماعة إجرامية منظمة، جماعة ذات هيكل تنظيمي مؤلفة من ثلاثة أشخاص فأكثر، موجودة لفترة من الزمن، وتعمل بصورة متظافرة بهدف ارتكاب واحد أو أكثر من الجرائم الخطيرة أو الأفعال المجرمة وفقا لهذه الإتفاقية من أجل الحصول بشكل مباشر أو غير مباشر على منفعة مالية أو منفعة مادية أخرى".

المطلب الأول: دور المنظمات الدولية العالمية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن منظمة الأمم المتحدة[1] تبذل جهودا لا يُستهان بها في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وتؤكد على ضرورة تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على التصدي لهذه الجرائم، حيث حظيت هذه الجريمة باهتمام مؤتمرات الأمم المتحدة وأبرز ما جاء في هذا المجال ما يلي[2]:

الفرع الأول: جهود الأمم المتحدة في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

انتهجت الأمم المتحدة استراتيجية متوازنة وشاملة ومتكاملة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، جسدتها من خلال عقد العديد من المؤتمرات الدولية في هذا الشأن، إضافة إلى اصدارها للعديد من القرارات المتتالية والمكملة لبعضها البعض.

فمن خلال هذا الفرع سنتطرق إلى المؤتمرات الدولية الأممية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (أولا)، القرارات الأممية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (ثانيا).

---

[1] أنشئت منظمة الأمم المتحدة بموجب معاهدة " سان فرانسيسكو" سنة 1945، يتكون ميثاقها من ديباجة و111 مادة، لهذه المنظمة ستة أجهزة رئيسية تعمل على تنفيذ أهدافها ومقاصدها كلا حسب اختصاصه وتتمثل في: مجلس الأمن، الجمعية العامة، المجلس الإقتصادي والإجتماعي، مجلس الوصاية، محكمة العدل الدولية، الأمانة العامة، إضافة إلى وجود العديد من الوكالات المتخصصة التابعة لها.

رابح نهائلي، قيرة سعاد، دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)، مجلة البحوث القانونية والإقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر، المجلد 04، العدد02، 2021، ص 128-129.

[2] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد2، 2015، ص 11.

أولا: المؤتمرات الدولية الأممية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

عقدت منظمة الأمم المتحدة العديد من المؤتمرات بغرض مناقشة التحديات والصعوبات المتعلقة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أهمها:

1 _ المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد في أوت 1990 بالعاصمة الكوبية هافانا:

بعد انعقاد مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين عام 1985 في مدينة ميلانو الإيطالية، والذي فيه تم التطرق إلى مشكلة الجرائم السيبرانية المرتكبة في الفضاء السيبراني، فمن بين التوجيهات الصادرة عنه تكليف لجنة الخبراء العشرين لدى منظمة الأمم المتحدة بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي، وهذه اللجنة بدورها أقرت مجموعة من التوصيات والمقترحات والمبادئ، التي تبناها المؤتمر الثامن لمكافحة الجريمة ومعاملة المجرمين المنعقد في أوت 1990 بالعاصمة الكوبية هافانا[1]، صدر عنه قرار متعلق بالجرائم ذات الصلة بالحاسوب، دعى فيه الدول الأعضاء إلى العمل على تكاثف جهودها لمكافحة الاستخدام السيء للحواسيب وتجريم هذه الأفعال جنائيا، وإلى اتخاذ مجموعة من الإجراءات إذا استدعت الضرورة ذلك، وتتمثل هذه الإجراءات في تحديث القوانين الموضوعية والإجرائية واتخاذ مختلف التدابير التي تضمن تطبيق القوانين الراهنة المتعلقة بسلطات التحقيق وقبول الأدلة في الإجراءات القضائية على الجرائم المعلوماتية، وتعديلها بتعديلات مناسبة، والنص كذلك على جرائم وجزاءات، وإجراءات تتعلق بالتحقيق والأدلة، لأنه من الضروري التصدي لهذا الشكل الجديد والمعقد

[1] الطيب بلواضح، الجريمة في الفضاء الإلكتروني في ظل التشريع الجزائري والفرنسي والتشريعات العربية، ط1، دار وائل للنشر والتوزيع، الأردن، 2020، ص 107-108.

من الإجرام في حالة غياب قوانين تنطبق عليه بشكل ملائم[1]، وأضافت توصيات أخرى تفتح أفاق جديدة للتعاون الدولي من خلال إرساء أو تطوير معايير دولية لأمن المعالجة الآلية للبيانات، ووضع تدابير ملائمة لحل مختلف الإشكالات التي تُثار في الجرائم المعلوماتية العابرة للحدود[2].

فيعتبر هذا المؤتمر بمثابة نقطة إنطلاق لتجريم الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والتصدي لسوء استخدام الحواسيب، ووضع تدابير التعاون الدولي، لأن هذه الجرائم لم تكن محل إهتمام على مستوى هيئة الأمم المتحدة.

وحوصلة ما توصل إليه هذا المؤتمر بخصوص إساءة إستخدام الحواسيب تكمن في ثلاث نقاط أساسية:

_ تجريم إساءة إستخدام الحواسيب

_ تطوير النظام القانوني في شقه الموضوعي والإجرائي ليتماشى مع هذه الجرئم المستحدثة

_ التعاون الدولي من خلال بلورة معايير دولية لأمن معالجة البيانات.

2_ مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة الجرمين 1995:

أوصى مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين، الذي تم انعقاده في القاهرة في عام 1995، بحماية الأفراد في خصوصيتهم وملكيتهم الفكرية من المخاطر المتزايدة للتكنولوجيا الحديثة، وبإلزامية التنسيق والتعاون بين أعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة[3].

---

[1] ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية، دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، المجلد1، العدد 1، 2009، ص 244-245.

[2] بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، د.ط، دار الخلدونية، الجزائر، 2017، ص116.

[3] محمود أحمد عبانه، جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص 159.

فهذا المؤتمر بدأ من نقطة نهاية المؤتمر الأول حيث حث على إلزامية التعاون الدولي لاتخاذ الاجراءات المناسبة، والمستجدات التي وردت في هذا المؤتمر تتمثل في حماية الخصوصية للأفراد وحماية الملكية الفكرية الذان لم يتم التطرق لهما في المؤتمر السابق.

3_ المؤتمر العاشر للأمم المتحدة لمنع الجريمة ومعاملة الجرمين 2000:

إنعقد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا من 10 إلى 17 أبريل 2000، وأثمر عنه إعلان فيينا بشأن الجريمة والعدالة مواجهة تحديات القرن الحادي والعشرين والذي بدوره إقترح توصيات بخصوص الجرائم المتعلقة بالحواسيب أي الجرائم المعلوماتية والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

والذي كان الهدف منه مكافحة الجريمة العالمية، كما أوصى المؤتمر العاشر الذي عقد في بودابست في سنة 2000، بإلزامية بذل جهود جادة للحد من زيادة جرائم تكنولوجيا المعلومات، التي تعتبر نموذجًا للجرائم الجديدة المستحدثة[1].

فهذا المؤتمر خلص إلى تصنيف الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من الجرائم العالمية، وتم اعتبارها من الجرائم المستحدثة التي تستوجب تكاثف الجهود لمكافحتها.

4_ مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة ومعاملة الجرمين 2010 بالبرازيل:

مشروع إعلان سلفادور بشأن الإستراتيجي ات الشاملة لمواجهة التحديات العالمية نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، ناقشت فيه الدول ببعض التعمق مختلف التطورات الأخيرة في استخدام تكنولوجيا المعلومات من طرف المجرمين والسلطات المختصة في مكافحة الجريمة، حيث تبقى منظمة الأمم المتحدة الاطار الأمثل لمكافحة

[1] محمود أحمد عبانه، المرجع السابق، ص 159.

الإجرام المتعلق بأنظمة المعالجة الآلية للمعطيات حيث وضعت مجموعة من القواعد الموضوعية والاجرائية لمواجهة هذا النوع من الإجرام[1].

ومن التوصيات الواردة في الإعلان بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات هي أن يقوم مكتب الأمم المتحدة المعني بالمخدرات والجريمة بتقديم المساعدة التقنية والتدريب إلى الدول من أجل تحسين تشريعاتها الوطنية، بغية التصدي للجريمة السيبرانية، بما في ذلك منع هذه الجريمة بكل أشكالها والكشف عنها والتحقيق فيها وملاحقة مرتكبيها قضائيا وتحسين أمن الشبكات الحاسوبية هذا ما ورد في البند 41 من تقريره، وبموجب البند 42 من تقرير هذا المؤتمر تمت دعوة لجنة منع الجريمة والعدالة الجنائية إلى النظر في دعوة فريق خبراء حكومي إلى الانعقاد من أجل إجراء دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص، واقتراح تدابير جديدة في هذا الشأن[2].

فأسفر هذا المؤتمر عن إقتراحات شاملة تحدد الجوانب الأساسية للجرائم السيبرانية من الناحية التقنية ومن الناحية التشريعية، وتضبط آليات التصدي لها من مختلف أعضاء المجتمع الدولي، وتم إدراج القطاع الخاص في هذا الشأن، عبر الشراكة بين القطاع العام والخاص وفواعل المجتمع الدولي.

---

[1] مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر، المجلد 12، العدد2، 2019، ص 707.

[2] القرار رقم 1 الذي اعتمده مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير،السلفادور، البرازيل، 12-19 نيسان/أبريل 2010، A/conf.213/18 ص 12- 13.

للاطلاع على وثيقة القرار منشورة على الموقع التالي:

https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_A.pdf

5 _ مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة ومعاملة الجرمين 2015 في دولة قطر:

ومن أبرز التوصيات التي وردت في المؤتمر بخصوص مكافحة الجرائم السيبرانية بمختلف أشكالها: ضرورة إستحداث آليات قانونية تجريمية وبرامج تتماشى مع الطبيعة الخاصة لهذا النوع من الجرائم لتسهيل عملية التوعية بخطورتها، ووضع تدابير الوقاية والمنع من وقوعها، وأساليب التحري بشانها، إضافة إلى اتخاذ مجموعة تدابير مستحدثة لأجل مكافحتها[1].

فهذا المؤتمر توصياته جاءت مغايرة لما جاءت به المؤتمرات السابقة له، حيث أورد مقاربات جديدة لم يتم إدراجها من قبل، فهو ركز على سياسة الوقاية والاستباقية لمكافحة هذه الجرائم قبل وقوعها وتحقق نتائجها، أي أن مُرتكزاته تمثلت في السياسة الوقائية.

وما يلاحظ على هذه المؤتمرات أنها جميعها أوصت بإرساء جملة من القواعد القانونية التشريعية بنوعيها الموضوعية والإجرائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات الواردت تحت أي مسمى سواء الجرائم السيبرانية أو الجرائم ذات الصلة بالحاسوب أو جرائم الخصوصية المعلوماتية، أو الجرائم المتعلقة بالحواسيب والمرتبطة بتكنولوجيات الاعلام والاتصال، أو جرائم تكنولوجيا المعلومات، والتي في مجملها يقصد بها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

فهذه المؤتمرات بتحليل توصيتها جميعا، يتضح لنا أنها رسمت معالم سياسة جنائية شاملة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، تضمنت الجانب الوقائي، والموضوعي والإجرائي، وأرست آليات مكافحتها من خلال التعاون الدولي بين أعضاء المجتمع الدولي، فأضحت هناك خطة واضحت وشاملة لمكافحة هذه الجرائم، إلا أنها تفتقر

[1] مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) – دراسة مقارنة، دار الخلدونية، الجزائر، 2018، ص269–272.

لطابع الإلزام الذي يترتب على مخالفته جزاء، وتفتقر كذلك لآليات التنفيذ والتطبيق الفعلي لهذه التوصيات.

ورغم ذلك فالتوصيات الناتجة عن هذه المؤتمرات تعتبر بمثابة إرهاصات لتوجيه السياسة التشريعة للدول وتطويرها مع مستجدات هذا النوع من الجرائم، ووضع رؤى استراتيجية لمقاربة شاملة للتصدي لها.

ثانيا: القرارات الأممية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

والقررات تُعرف أنها: " تعبير عن إرادة المنظمة موجهة إلى جهة أو عدة جهات متضمنة المبادرة لاتخاذ سلوك معين"[1]، وكون الجرائم السيبرانية بصفة عامة والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أصبحت من أبرز الاهتمامات العالمية فالجمعية العامة لهيئة الأمم المتحدة أصدرت بشأنها العديد من القرارات، وبطبيعة الحال فهذه القررات تساهم بشكل كبير في تطوير القانون الدولي العرفي والاتفاقي، أصدرت الجمعية العامة[2] العديد من القرارات[3] بخصوص الجرائم السيبرانية بصفة عامة دون الاقتصار على نوع محدد منها،

[1] عصموني خليفة، مكانة قرارات المنظمات الدولية بين مصادر القانون الدولي العام، مجلة السياسة العالمية، مخبر الدراسات السياسية والدولية، جامعة امحمد بوقرة بومرداس، الجزائر، المجلد 05، العدد02، 2021، ص506.

[2] وفقا لنص المادة 09 من ميثاق الأمم المتحدة الصادر بتاريخ 26 جوان 1945، بسان فرانسيسكو بالولايات المتحدة الامريكية، (تاريخ النفاذ: 24 أكتوبر 1945)، فإن الجمعية العامة تتكون من كل الدول الأعضاء في هيئة الأمم المتحدة، وتتساوى هذه الدول في التصويت.

حيث تنص المادة 09 من ميثاق الأمم المتحدة: " 1- تتألف الجمعية العامة من جميع أعضاء "الأمم المتحدة"
2 – لا يجوز أن يكون للعضو الواحد أكثر من خمسة مندوبين في الجمعية العامة".

[3] وما يجدر بنا الإشارة إليه في هذا الصدد أن قرارات الجمعية العامة تنقسم إلى قسمين:

1- قرارات ليست لها أي آثار قانونية وغير ملزمة.

2- قرارات لها آثار قانونية وتكون ملزمة في مواجهة المخاطبين بها وعلى الدول الأعضاء الالتزام بما جاء فيها ومثالها:

- قرارات إدارية تتعلق بضم أو طرد عضو بناء على توصية من مجلس الأمن.
- إقرار أو تحديد ميزانية المنظمة وتحديد حصة كل دولة فيها.

وأكدت المادة 10[1] من ميثاق الأمم المتحدة أن القرارات الصادرة عن الجمعية العامة لها صفة التوصيات وهي ليست ملزمة للدول ولا تفرض أي إلتزام قانوني، وجل الإجراءات التي تصدر من طرف الجمعية العامة ليست لها إلا صفة التوصية وليس من شأنها أن تولد إلتزامات قانونية على الدول الأعضاء في المنظمة فتصرفات الجمعية العامة غير ملزمة وليس لها حق مناقشة إلا بعض المسائل، فتصرفاتها ليست ذات قيمة قانونية، فعدم الإعتراف بأي قوة ملزمة للتوصيات الصادرة عن الجمعية العامة إلا ما جاء في الأعمال التحضيرية لميثاق الأمم المتحدة[2]، ويعتبر هذا الرأي السائد في الفقه[3]، إلا أنه يوجد رأي معارض[4] له ويقر بإلزامية القرارات الصادرة عن الجمعية العامة.

- انتخاب الأعضاء الدائمين في مجلس الأمن
- القرارات التي تهدف إلى تأكيد مبادئ قانونية عامة أو قواعد عرفية.

محمد الصغير سليني، قرارات المنظمات الدولية ودورها في إرساء قواعد القانون الدولي، أطروحة لنيل شهادة دكتوراه علوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة يحي فارس المدية، الجزائر، نوقشت بتاريخ 2021/02/01، ص135-136.

[1] المادة 10 من ميثاق الأمم المتحدة: " للجمعية العامة أن تناقش أية مسألة أو أمر يدخل في نطاق هذا الميثاق أو يتصل بسلطات فرع من الفروع المنصوص عليها فيه أو وظائفه. كما أن لها في ماعدا ما نص عليه في المادة 12 أن توصي أعضاء الهيئة أو مجلس الأمن أو كليهما بما تراه في تلك المسائل والأمور"

[2] مبخوتة أحمد، الوظيفة التشريعية للجمعية العامة وأثرها على تطور قواعد القانون الدولي المعاصر، مجلة القانون، معهد العلوم القانونية والادارية، المركز الجامعي أحمد زبانة بغليزان، الجزائر، المجلد 07، العدد 02، 2018، ص 147-148.

[3] وقد برر هذا الرأي موقفه بما ورد في الأعمال التحضيرية لميثاق الأمم المتحدة، حيث أن هذا الاتجاه السائد نفى الصفة الإلزامية للتوصيات الصادرة عن الجمعية العامة، وتم تأكيد ذلك خلال مؤتمر "سان فرانسيسكو" عندما تعرضت اللجنة إلى الفرع (ب) من الفصل الخامس لمخطط "دامبرون أوكس" صوتت سلبا على سؤال يتعلق بحق الجمعية العامة للأمم المتحدة في إصدار قواعد وقررات ملزمة للدول الأعضاء.

للتفصيل أكثر أنظر: مبخوتة أحمد، القيمة القانونية للقرارات والتوصيات الصادرة عن الجمعية على ضوء أحكام القانون الدولي المعاصر، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 3، العدد 1، 2010، ص120.

[4] يستند هذا الرأي على أنه ليس من الضروري التمييز بين مختلف الأعمال الصادرة عن الجمعية (قرارات، توصيات...) من حيث القوة الإلزامية.

ومن القرارات الصادرة عن الجمعية العامة للأمم المتحدة بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

1_ القرار رقم 45/95 المتضمن المبادئ التوجيهية للأمم المتحدة:

تم إقرار مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبات الإلكترونية، واعتمدت ونشرت بموجب قرار الجمعية العامة للأمم المتحدة 95/ 45 المؤرخ في 14 كانون الأول/ ديسمبر 1990[1]، ونظمت هذه المبادئ جُل مسائل الحماية[2]، وبينت نطاق تطبيق هذه المبادئ حيث تُطبق على جُل الملفات المعالجة آليا أو يدويا سواء العامة أو الخاصة، وحثت على وضع أحكام خاصة اختياريا من قبل الدول بغرض توسيع نطاق تطبيق هذه المبادئ، لتشمل الحماية كل الأشخاص الطبيعيين والمعنويين، وورد فيها أن هذه المبادئ كذلك يمكن تطبيقها على البيانات ذات الطابع الشخصي التي تحتفظ بها المنظمات الحكومية الدولية[3]، وتطرقت كذلك هذه المبادئ إلى الجهات المعنية بجمع البيانات الشخصية بنوعيها عامة وخاصة، وتضمنت مجمل مسائل الحماية على المستوى الوطني، ونصت على المبادئ الواجب إقرارها، والإستثناءات الواردة على هذه المبادئ، ودعت إلى

وأن للقرارات والتوصيات الصادرة عن الجمعية العامة قوة أدبية وسياسية كبيرة تجعل أي دولة متترددة في المجاهرة صراحة بأنها تعارض ما جاء في قرار صادر عن أغلبية الدول أي أعضاء الهيئة، لتدفع عن نفسها تهمة مخالفة قرار الجماعة الدولية، للتفصيل أكثر أنظر: محمد الصغير سليني، المرجع السابق، ص137.

[1] مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

[2] منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية: الهمّ الأمني وحقوق الأفراد، ط1، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العرب، جامعة الدول العربية، بيروت، لبنان، 2018، ص 52.

[3] مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/95المؤرخ في 14 كانون الأول/ديسمبر 1990.

ضرورة تعيين سلطات مخولة لمراقبة تطبيق هذه المبادئ وإقرار العقوبات الجزائية على المستوى الدولي، ونظمت تدفق البيانات عبر الحدود[1].

وبخصوص المبادئ التي تنص على ضمانات دنيا يجب إدخالها في التشريعات الوطنية في قوانين الدول الأعضاء المعنية هي:

الإلتزام بمبدأ المشروعية والنزاهة[2]، ومبدأ الدقة[3]، ومبدأ تحديد الغاية ولابد من التوافق بين مدة الحفظ ومدة بلوغ تلك الغاية[4]، ومبدأ وصول الأشخاص المعنيين إلى الملفات الذي أقر حق الشخص المعني بالمعالجة في الإطلاع عن كيفية التصرف ببياناته وكيفيات إستخدامها، وإلى حقه في الإعلام، وحقه في تصحيح بياناته أو محوها[5]، ومبدأ عدم التمييز حيث أقر بأنه لا يجوز تسجيل البيانات التي تؤدي إلى التمييز وعلى وجه الخصوص الحساسة منها، ومبدأ الأمن الذي يقر بضرورة توفير التدابير المناسبة لحماية الملفات المحتوات على هذه البيانات من التلف والفقدان بسبب المخاطر الطبيعية، أو البشرية بسبب الاطلاع عليها

[1] منى الأشقر جبور، محمود جبور، المرجع السابق، ص52.

[2] مبدأ الشرعية: حيث وفقا لهذا المبدأ لا ينبغي الحصول على البيانات المتعلقة بالأفراد أو معالجتها بوسائل غير مشروعة أو غير عادلة، أو استخدامها لأغراض تتعارض مع مقاصد ميثاق الأمم المتحدة ومبادئه. أنظر: مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

[3] مبدأ الدقة: ينبغي أن يُطلب من الأشخاص المسؤولين عن إنشاء ملف أو عن تنفيذه التحقق من دقة البيانات المسجلة ومدى ملاءمتها وضمان بقائها كاملة قدر الإمكان لتفادي الأخطاء عن طريق الإغفال واستكمالها، بصفة دورية أو عند استخدام المعلومات الواردة في الملف، ما دام يجري تجهيزها. أنظر: مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

[4] مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

[5] منى الأشقر جبور، محمود جبور، المرجع نفسه ، ص 53.

واستخدامها بطريقة غير مشروعة وغير آمنة، وتم تحديد الإستثناءات الواردة على هذه المبادئ على سبيل الحصر[1].

والسؤال المطروح هنا بشأن هذه المبادئ التوجيهية، هو هل هي ملزمة بمثابة الإتفاقية أم لا؟ وإجابة على هذا السؤال فالقرار السالف الذكر نص على المبادئ المتعلقة بالضمانات الدنيا التي ينبغي النص عليها في التشريعات الوطنية لكل دولة، فهذه المبادئ التوجيهية هي مبادئ غير ملزمة لأنها مجرد توصيات للدول الأعضاء لأجل النص عليها في نصوصها وتشريعاتها الداخلية الوطنية[2].

2_ القرارات تحت عنوان التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي:

أصدرت الجمعية العامة للأمم المتحدة العديد من القرارات تحت عنوان التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي على مدار سنوات حيث كانت قراراتها كالتالي:

أ_ القرار رقم 53/ 70 المؤرخ في 4 كانون الأول/ ديسمبر 1998:

أعربت فيه الجمعية العامة عن قلقها المحتمل حول استخدام إستخدام هذه التكنولوجيات المستحدثة لتحقيق أهداف تتعارض وحماية الأمن والسلم الدوليين والتي يمكن أن تؤثر سلبا على أمن الدول، حيث رأت أنه من الضروري منع إساءة إستخدام هذه التكنولوجيات لتحقيق أغراض إجرامية وإرهابية، حيث طلبت من الدول الأعضاء النظر إلى مختلف التهديدات القائمة حاليا والمحتملة مستقبلا في مجال أمن المعلومات، وطلبت من الدول الأعضاء أن

[1] مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة 45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

[2] بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي سعيدة، الجزائر، العدد 6، جوان 2016، ص 281.

تبلغ الأمين العام بآرائها وتقييماتها بشأن عدة مسائل منها: التفهم العام لقضايا أمن المعلومات، وتعريف المفاهيم الأساسية المتصلة بأمن المعلومات باعتبارها مفاهيم مستحدثة، إضافة إلى وضع مبادئ دولية تعزز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية وتساعد في مكافحة الإرهاب والإجرام المتصل بالمعلومات1.

بخصوص ما ورد في هذا القرار فقد ركز على أمن الأنظمة المعلوماتية وحمايتها من كل أشكال التهديد، وايجاد تعريف للمصطلحات والمفاهيم المرتبطة بها، ويعتبر هذا أول قرار ربط الاستخدام السيء لتكنولوجيا المعلومات بالجرائم الارهابية.

ب_ القرار رقم 53/ 49 المؤرخ في 1 ديسمبر 1999:

هذا القرار رأت فيه الجمعية أن التقييمات التي قام بها الأعضاء والتي وردت في تقرير الأمين العام واجتماع الخبراء الدولي أسهما في زيادة تفهم جوهر القضايا المتعلقة بأمن المعلومات على الصعيد الدولي وما يتصل به من مفاهيم والتدابير الممكن اتخاذها للحد مما يلوح من التهديدات في هذا الميدان، ودعت جميع الدول الأعضاء إلى مواصلة إبلاغ الأمين العام بآرائها وتقييمها في المسائل التي سبق تقييمها[2].

ج_ القرار رقم 55/ 28 المؤرخ في 20 نوفمبر 2000:

دعت كل الدول الأعضاء إلى مواصلة إبلاغ الأمين العام بوجهات نظرها وتقييماتها لمسائل أمن المعلومات، وتحديد مختلف المفاهيم الأساسية المتعلقة بأمن المعلومات[3].

[1] قرار الجمعية العامة رقم 53/ 70، التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 63، من جدول أعمال الدورة 53، المؤرخ في 4 كانون الأول/ ديسمبر 1998.

[2] قرار الجمعية العامة رقم 53/ 49، التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، المؤرخ في 1 ديسمبر 1999.

[3] قرار الجمعية العامة رقم 55/ 28 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 68 من جدول أعمال الدورة 55، المؤرخ في 20 نوفمبر 2000.

وما يلاحظ أن هذا القرار وسابقه لم يأتيا بجديد، وإنما كان مكملين للقرار السابق لهما رقم 53/ 70، وهذا بغرض ضبط وتحديد المفاهيم والمصطلحات المتعلقة بأمن أنظمة المعلومات، وفهم فحوها وكل مايتعلق بها.

د_ القرار رقم 56/ 19 المؤرخ في 29 نوفمبر 2001:

طلبت فيه من الأمين العام أن يقوم بدارسة الأخطار القائمة والمحتملة في مجال أمن المعلومات، وتدابير التعاون التي يمكن أن يتم اتحاذها للتصدي لها، وأن يقوم بإجراء دراسة للمفاهيم السالفة الذكر بمساعدة فريق من الخبراء الحكوميين، بتعاون مع الدول الأعضاء القادرة على تقديم تلك المساعدة، وأن يقدم تقرير عن نتائج الدراسة إلى الجمعية في دورتها رقم 60 وقررت إدراج في جدول أعمال الدورة الموالية (الدورة 57) بند معنون "بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي"[1].

هـ_ القرار رقم 57/ 53 المؤرخ في 22 نوفمبر 2002:

تضمن نفس محتوى القرار السابق، أعادت تقديم نفس الطلب الذي قدمته في القرار السابق للأمين العام بغرض دراسة الأخطار القائمة والمحتملة في مجال أمن المعلومات، وقررت إدراجها في جدول أعمالها لدورتها الموالية (الدورة 58) البند المعنون "بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي"[2].

[1] قرار الجمعية العامة رقم 56/ 19 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 69 من جدول أعمال الدورة 56، المؤرخ في 29 نوفمبر 2001.

[2] قرار الجمعية العامة رقم 57/ 53 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 61 من جدول أعمال الدورة 57، المؤرخ في 29 نوفمبر 2001.

و_ القرار رقم 58/ 32 المؤرخ في 8 ديسمبر 2003:

تضمن هذا القرار نفس أحكام القرار السابق له، إلا أنه أضاف أن الجمعية العامة دعت الدول الأعضاء إلى مواصلة النظر، على الصعيد المتعدد الأطراف، في التهديدات القائمة والمحتملة في ميدان أمن المعلومات، والتدابير الممكنة للحد من المخاطر في هذا المجال بما يتوافق والحاجة إلى الحفاظ على التدفق الحر للمعلومات.

وترى أن الهدف من هذه التدابير يمكن تحقيقه بدراسة المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات السلكية واللاسلكية، وقررت أن تدرج في جدول أعمال دورتها المقبلة (الدورة 59) البند المعنون "بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي"[1].

ز_ القرار رقم 59/ 61 المؤرخ في 3 ديسمبر 2004:

تضمن ما سبق الإشارة إليه في القرار السابق، إلا أن ما لاحظته الجمعية العامة أن الأمين العام يدرس في الأخطار القائمة والمحتملة في مجال أمن المعلومات والتدابير الرامية للتصدي لها، وأنه يقوم بإجراء دراسة للمفاهيم الواردة في الفقرة 2 من هذا القرار، وذلك بمساعدة الخبراء الحكوميين، وأنه سيقدم تقرير عن نتائج هذه الدراسة الى الجمعية العامة في دورتها القادمة، وتم عقد الدورة الاولى في الفترة من 12 إلى 16 تموز/ يوليه 2004 في نيويورك من طرف فريق الخبراء الذي أنشأه الأمين العام، واعتزم عقد دورتين في سنة 2005 للاضطلاع بولايته المحددة في القرار السابق لهذا القرار، وقرر إدارج بند " التطورات

[1] قرار الجمعية العامة رقم 58/ 32 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 68 من جدول أعمال الدورة 58، المؤرخ في 8 ديسمبر 2003.

في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي" ضمن جدول الأعمال المؤقت لدورتها القادمة رقم الستين[1].

ح- القرار رقم 60/ 45 المؤرخ في 8 ديسمبر 2005:

تضمن نفس ما جاء في القرار السابق، إلا أن الجمعية العامة لاحظت إسهام الدول الأعضاء التي قدمت إلى الأمين العام تقييماتها للمسائل التي تتصل بأمن المعلومات المنصوص عليها في الفقرات من 1 إلى 3 من القرارات السابقة المتمثلة في القرار 53/ 70، القرار 54/ 49، 55/ 28، 56/ 19، 57/ 53، 58/ 32، 59/ 61[2]. وتوالت القرارات التي تكمل بعضها البعض في هذا الشأن كما يلي:

ط_ القرار رقم 17/62 المؤرخ في 5 ديسمبر 2007[3].

ك _ القرار رقم 63/ 37 المؤرخ في 2 ديسمبر 2008[4].

ل_ القرار رقم 64/ 25 المؤرخ في 2 ديسمبر 2009[5].

م_ القرار رقم 65/ 31 المؤرخ في 8 ديسمبر 2010[6]

---

[1] قرار الجمعية العامة رقم 59/ 61 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 60 من جدول أعمال الدورة 59، المؤرخ في 3 كانون الأول/ ديسمبر 2004.

[2] قرار الجمعية العامة رقم 60/ 45 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 86 من جدول أعمال الدورة 60، المؤرخ في 8 كانون الأول/ ديسمبر 2005.

[3] قرار الجمعية العامة رقم 17/62 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 62، المؤرخ في 5 كانون الأول/ ديسمبر 2007. على الرابط التالي:

[4] قرار الجمعية العامة رقم 63/ 37 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 85 من جدول أعمال الدورة 63، المؤرخ في 2 كانون الأول/ ديسمبر 2008.

[5] قرار الجمعية العامة رقم 25/64 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 91 من جدول أعمال الدورة 64، المؤرخ في 2 كانون الأول/ ديسمبر 2009.

[6] قرار الجمعية العامة رقم 65/ 41 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 85 من جدول أعمال الدورة 65، المؤرخ في 8 كانون الأول/ ديسمبر 2010.

ن_ القرار رقم 66/ 24 المؤرخ في 2 ديسمبر 2011[1].

س_ القرار رقم 67/ 27 المؤرخ في 3 ديسمبر 2012[2].

ع_ القرار رقم 68/ 243 المؤرخ في 27 ديسمبر 2013[3].

ف_ القرار رقم 69/ 28 المؤرخ في 2 ديسمبر 2014[4].

ص_ القرار رقم 70/ 237 المؤرخ في 23 ديسمبر 2015[5].

ق_ القرار رقم 71/ 28 المؤرخ في 5 ديسمبر 2016[6].

ر_ القرار رقم 73/ 27 المؤرخ في 5 ديسمبر 2018[7].

---

[1] قرار الجمعية العامة رقم 66/ 24 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 66، المؤرخ في 2 كانون الأول/ ديسمبر 2011.

[2] قرار الجمعية العامة رقم67/ 27 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 89 من جدول أعمال الدورة 67، المؤرخ في 3 كانون الأول/ ديسمبر 2012.

[3] قرار الجمعية العامة رقم68/ 243 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 94 من جدول أعمال الدورة 68، المؤرخ في 27 كانون الأول/ ديسمبر 2013.

[4] قرار الجمعية العامة رقم 69/ 28 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 91 من جدول أعمال الدورة 69، المؤرخ في 2 كانون الأول/ ديسمبر 2014.

[5] قرار الجمعية العامة رقم 70/ 237 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 92 من جدول أعمال الدورة 70، المؤرخ في 23 كانون الأول/ ديسمبر 2015.

[6] قرار الجمعية العامة رقم 71/ 27 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 71، المؤرخ في 2 كانون الأول/ ديسمبر 2016.

[7] قرار الجمعية العامة رقم 73/ 27 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 96 من جدول أعمال الدورة 73، المؤرخ في 5 كانون الأول/ ديسمبر 2018.

3_ القرارات الموسومة ب: تعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية ولاسيما قدراته في مجال التعاون التقني

حيث أن جل هذه القرارات تهتم بالتعاون التقني في مجال القرصنة والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وبإجراءات مكافحة هذه الجرائم، وإجراءات الوقاية الاستباقية، وتعزيز التعاون الدولي بشأنها وهذه القرارات جاءت كما يلي:

أ_ القرار رقم 66/ 181 المؤرخ في 19 ديسمبر 2011[1].

ب_ القرار رقم 68/ 193 المؤرخ في 18 ديسمبر 2013[2].

ج_ القرار رقم 72/ 196 المؤرخ في 19 ديسمبر 2017[3].

4_ القرارات الموسومة ب: مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

أ_ القرار رقم (55/ 63) المؤرخ في 04/ 12/ 2000:

جاء هذا القرار بالعديد من التدابير بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية والتي أهمها تتمثل فيما يلي: تنسيق كل الدول المعنية التعاون في مجال القضايا الدولية المتعلقة باستخدام تكنولوجيا المعلومات لأغراض إجرامية، وتبادلها المعلومات المتعلقة بالصعوبات التي تواجهها في مكافحة إساءة استعمال تكنولوجيا المعلومات، وينبغي تدريب العاملين في مجال الأمني والقضائي بما يمكنهم من مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وينبغي سن نظم قانونية تحمي سرية البيانات ونظم

[1] قرار الجمعية العامة رقم 66/ 181 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 107 من جدول أعمال الدورة 66، المؤرخ في 19 كانون الأول/ ديسمبر 2011.

[2] قرار الجمعية العامة رقم 68/ 193 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 108 من جدول أعمال الدورة 68، المؤرخ في 18 كانون الأول/ ديسمبر 2013.

[3] قرار الجمعية العامة رقم 72/ 196 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 107 من جدول أعمال الدورة 72، المؤرخ في 19 كانون الأول/ ديسمبر 2017.

المعالجة الآلية للمعطيات وتعاقب من يسيء استعمالها لأغراض إجرامية، وينبغي توعية عامة الناس بضرورة منع إساءة الاستعمال والكشف عنها وتعقب المجرمين وجمع الأدلة، ووضع حلول تحمي حريات الأفراد وحياتهم الخاصة[1].

وماتمت ملاحظته بخصوص هذا القرار أنه جاء بأهم آليات مكافحة هذه الجرائم على المستوى الدولي من تعاون دولي وتبادل المعلومات بين الدول، وكذلك أورد أهم إجراءات الوقاية من هذه الجرائم والمتمثلة في تدريب العنصر البشري لمكافحة هذه الجرائم في المجالين الأمني والقضائي، والتوعية بخطورة هذه الجرائم، والكشف عنها، وصولا إلى سن تشريعات تجرمها وتعاقب على ارتكابها، وحمي حريات الأفراد والحياة الخاصة بهم.

ب_ القرار رقم (56/ 121) المؤرخ في 12/19/ 2001:

حيث أهم ما ورد في هذا القرار هو دعوة الجمعية العامة الدول الأعضاء فيها، عند وضعهم سياسات وقوانين وممارسات وطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، أن تأخذ بعين الاعتبار مختلف أعمال وإنجازات لجنة منع الجريمة والعدالة الجنائية، وكذلك المنظمات الدولية والاقليمية الأخرى التي تسعى لمكافحة هذه الجرائم[2].

ج- القرار رقم 61/ 54 المؤرخ في 6 ديسمبر2006[3].

د_ القرار رقم 73/ 187 المؤرخ في 17 ديسمبر2018[1].

[1] قرار الجمعية العامة رقم 55/ 63 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 105 من جدول أعمال الدورة 55، المؤرخ في 4 كانون الأول/ ديسمبر 2000. على الرابط التالي:

[2] قرار الجمعية العامة رقم 56/ 121 المعنون بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 110 من جدول أعمال الدورة 56، المؤرخ في 19 كانون الأول/ ديسمبر 2001 على الرابط التالي:

[3] قرار الجمعية العامة رقم 61/ 54 المعنون بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، المؤرخ في6 ديسمبر2006.

هـ_ القرار رقم 74/ 247 المؤرخ في 27 ديسمبر 2019[2]:

بتاريخ 27 ديسمبر 2019 اتخذت الجمعية العامة القرار رقم 74/ 247، بناءً على ملاحظتها للارتفاع الهائل لمستوى الجرائم وبالمقابل ارتفاع درجات تعقيدها في العالم الرقمي وتنوعها، وهذا راجع لاستخدام المجرمين لتكنولوجيات الإعلام والاتصال، وكذلك تخوفها من الخطر المحتمل لإساءة استخدام التكنولوجيات المستحدثة الناشئة بما فيها الذكاء الاصطناعي، وأكدت الجمعية على ضرورة تعزيز التنسيق والتعاون بين الدول بهدف مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الاجرامية، ولاسيما من خلال تقديم المساعدة التقنية إلى البلدان النامية بناءً على طلبها من أجل تحسين التشريعات وأطر العمل الوطنية وبناء قدرات السلطة الوطنية من أجل مكافحة هذا الاستخدام غير المشروع بكل أشكاله، بما في ذلك البحث والتحري والتحقيق فيه وملاحقة مرتكبيه قضائيا، إذ تؤكد في هذا السياق على الدور البارز للأمم المتحدة في هذا الشأن، وخصوصا لجنة الجريمة والعدالة الجنائية، ووفقا للقرار رقم 4/26 المؤرخ في 26 ماي 2017 أعربت فيه اللجنة عن تقديرها للعمل الذي يقوم به فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية وطلبت من فريق الخبراء مواصلة عمله بهدف إيجاد الخيارات المتاحة بغرض تعزيز التدابير الشاملة القانونية أو غيرها من التدابير على المستويين الوطني والدولي القانونية لمكافحة الجريمة السيبرانية وتقديم اقتراحات في شكل تدابير مستحدثة في هذا الصدد، أعادت التأكيد من جديد على الدور البارز لمكتب الأمم المتحدة المعني بالمخدرات والجريمة. وقررت إنشاء لجنة

[1] قرار الجمعية العامة رقم 73/ 187 المعنون بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 109 من جدول أعمال الدورة 73، المؤرخ في 17 كانون الأول/ ديسمبر 2018.

[2] قرار الجمعية العامة رقم 74/ 247 المعنون بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 107 من جدول أعمال الدورة 74، المؤرخ في 27 كانون الأول/ ديسمبر 2019.

خبراء حكومية دولية مخصصة[1]، لأجل وضع اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، حيث يجب مراعاة كافة الصكوك الدولية الجهود المبذولة في الوقت الحالي على كل من المستوى الدولي والاقليمي والوطني بخصوص استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وكذلك مراعاة الأعمال والنتائج المتوصل إليها من طرف الفريق الحكومي المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، وقررت أن يتم إدراج البند الموسوم ب "مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية" في جدول أعمالها المؤقت للدورة الموالية رقم 75. وفي ديسمبر 2019 تم تصويت الجمعية العامة للأمم المتحدة لبدء التفاوض على معاهدة الأمم المتحدة ومعاهدة الأمم المتحدة بشأن الجرائم الإلكترونية[2].

وما يجدر بنا الإشارة إليه أنه على المستوى الدولي لحد الآن لا توجد اتفاقية دولية عالمية خاصة بمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ويمكن تطبيق اتفاقية الجريمة المنظمة التي لها طابع دولي على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات إذا اتخذت شكل الجريمة المنظمة العابرة للحدود الوطنية.

و_ القرار رقم 75/ 282 المؤرخ في 26 ماي 2021:

أهم ما جاء في هذا القرار أن الجمعية العامة رحبت بانتخاب أعضاء مكتب اللجنة المخصصة لصياغة اتفاقية دولية شاملة بشأن مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية في دورتها التنظيمية المعقودة في 10 مايو 2021، وقررت مواصلة العمل من قِبل مكتب الأمم المتحدة المعني بالمخدرات والجريمة والذي يعتبر أمانة

[1] لجنة الخبراء الحكومية المخصصة: تكون مفتوحة العضوية، للأعضاء من كل تمثل الأقاليم، قرار الجمعية العامة رقم 74/ 247 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 107 من جدول أعمال الدورة 74، المؤرخ في 27 كانون الأول/ ديسمبر 2019.

[2] Official United Nations website. available at: https://unric.org/en/a-un-treaty-on-cybercrime-en-route/. accessed April 10, 2023 At10 :00.

اللجنة المخصصة، وأكدت كذلك على أن اللجنة المخصصة يجب عليها مراعاة جميع الصكوك الدولية والجهود الوطنية والإقليمية والدولية لمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، وبالخصوص أعمال ونتائج فريق الخبراء الحكومي الدولي المكلف بإجراء دراسة متعمقة حول الإجرام السيبراني[1].

5_ قرارات الأمم المتحدة بشأن الخصوصية في العصر الرقمي:

أ_ قرار الجمعية العامة للأمم المتحدة بشان الخصوصية في العصر الرقمي رقم (68/167):

بناء على تقرير اللجنة الثالثة بتاريخ 18 كانون الأول/ ديسمبر2013، أصدرته الجمعية العامة للأمم المتحدة، حيث تأكد فيه أن "الحق في الخصوصية، لا يسمح بتعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أو في شؤون أسرته أو في بيته أو مرسلاته، وحقه في التمتع بحماية القانون، من مثل هذا التدخل على النحو المبين في المادة 12 من الإعلان العالمي لحقوق الإنسان، والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية"[2]، وطلبت الجمعية العامة من مفوضة الأمم المتحدة السامية لحقوق الإنسان تقديم تقرير بشأن ضمان حماية الحق في الخصوصية، عند اعتراض ومراقبة الاتصالات وجمع المعطيات الشخصية على الصعيد الوطني والدولي، إليها وإلى مجلس حقوق الإنسان في دورتهما الموالية[3].

[1] قرار الجمعية العامة رقم 75/ 282 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 112 من جدول أعمال الدورة 75، المؤرخ في 26 أيار/ مايو 2021.

[2] قرار الجمعية العامة رقم 68/ 167 المعنون بالحق في الخصوصية في العصر الرقمي، البند 69 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الأول/ ديسمبر 2013.

[3] قرار الجمعية العامة رقم 68/ 167 المعنون بالحق في الخصوصية في العصر الرقمي، البند 69 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الأول/ ديسمبر 2013.

ب_ تقرير الحق في الخصوصية في العصر الرقمي لعام 2014:

اتخذت الجمعية العامة القرار رقم 166/69 بتاريخ كانون الأول/ ديسمبر 2014 بشأن الحق في الخصوصية في العصر الرقمي، أكدت فيه مجددا على هذا الحق، وحظرت المساس به، ولاحظت أن هناك بيانات وصفية يمكنها أن تؤدي إلى الكشف عن المعلومات الشخصية، وأكدت على وجوب احترام الدول للمواثيق الدولية الملتزمة بها والمتعلقة بحقوق الانسان[1].

وورد في هذا القرار العديد من التوصيات التي كلها تدعو إلى إحترام الحق في الخصوصية، والحد من انتهاكه، وإعادة النظر في القوانين المتعلقة بجمع البيانات الشخصية، وإجراءات المراقبة الإلكترونية للاتصالات، وفرض رقابة قضائية وإدارية عليها[2].

_القرار رقم 179/73 بشأن الحق في الخصوصية في العصر الرقمي: قرار اتخذته الجمعية العامة 17 ديسمبر 2018[3].

وتبعا لذلك، نلاحظ أن جل هذه القرارات وردت بشكل متتالي ومكملة لبعضها البعض مست الشقين الموضوعي والإجرائي وكذلك شق المنع والوقاية، وانصبت على مختلف أنواع الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بداية من ظهورها في شكل بسيط إلى غاية تطورها واتخاذ أشكالها الحالية من مختلف الأفعال الإجرامية المتمثلة في إساءة إستخدام التكنولوجيات لتحقيق أغراض إجرامية وإرهابية، والإعتداءات على المعطيات الشخصية والإعتداءات على الخصوصية الرقمية، فهذه القرارات وضعت حجر الأساس ل

[1] قرار الجمعية العامة رقم 69/ 166 المعنون بالحق في الخصوصية في العصر الرقمي، البند 68 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الأول/ ديسمبر 2014.

[2] قرار الجمعية العامة رقم 69/ 166 المعنون ب الحق في الخصوصية في العصر الرقمي، البند 68 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الأول/ ديسمبر 2014.

[3] قرار الجمعية العامة رقم 73/ 179 المعنون ب الحق في الخصوصية في العصر الرقمي، البند 74 (ب) من جدول أعمال الدورة 73، الصادر بتاريخ 17 كانون الأول/ ديسمبر 2018.

"مشروع اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية"، والتي أوردت أنواع جديدة للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي نتجت عن التوسع في استخدام تكنولوجيات الاعلام والإتصال.

الفرع الثاني: دور المنظمات المتخصصة التابعة للأمم المتحدة في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

للوكالات المتخصصة التابعة لمنظمة الأمم المتحدة كذلك دور مهم في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث تعتبر منظمات تعمل مع الأمم المتحدة، ومن خلال هذا الفرع سنتطرق إلى أبرز هذه المنظمات والمتمثلة في الاتحاد الدولي للاتصالات (ITU) (أولا)، و المنظمة العالمية للملكية الفكرية (ثانيا).

أولا: الاتحاد الدولي للاتصالات (ITU)

اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم (45) الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلوماتي ومكافحة الرسائل الاقتحامية، وقد تبنى مجموعة من التوصيات في مجال الأمن المعلوماتي والرسائل، كما أطلق الأمين العام للاتحاد في أيار 2007، جدول أعمال الأمن المعلوماتي العالمي لوضع إطار لمواجهة التحديات المتزايدة لأمن الانترنت، ولإيجاد حلول لتعزيز الثقة والأمن في مجتمع المعلومات، وفي أكتوبر 2007 أنشئ فريق من الخبراء رفيع المستوى (HLEG) ضم أكثر من مائة خبير قدموا التقارير والتوصيات في حزيران 2008، حيث نشرت الإستراتيجية العالمية في 2008/11/12، وقد اشتملت هذه الإستراتيجية على المجالات التالية: التدابير القانونية والتدابير التقنية والإجرائية، والهياكل التنظيمية، وبناء القدرات، والتعاون الدولي[1].

[1] عبد الإله النوايسية، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمان، الأردن، 2017، ص52.

وقد تبدو الاستراتيجية التي اعتمدها الاتحاد الدولي للاتصالات شاملة، لكنها لا تسلط الضوء بشكل كاف على تحديات الأمن السيبراني من جميع جوانبها، ولم تفصل فيها بشكل تام، ولم تحدد نوعها إذا ما كانت هجمات سيبرانية، أو تصيد إحتيالي، أو قرصنة، أو مساس بالخصوصية أو سرية البيانات...الخ.

ثانيا: المنظمة العالمية للملكية الفكرية

هي منظمة دولية حكومية من بين الوكالات المتخصصة التابعة للأمم المتحدة، هدفها الأساسي تشجيع النشاط الابتكاري، وتطوير مجال حماية الملكية الصناعية وحماية المصنفات الأدبية والفنية، إضافة إلى اهتمامها بمجال المعلوماتية من خلال توفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، وتجسيد هذه الحماية من خلال الاتفاقيات العالمية وخاصة اتفاقية "التريبس" و"اتفاقية بيرن"، اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير قوانينها الداخلية ، وخاصة التي تتعلق بحقوق المؤلف، كما أن هذه الآليات الاتفاقية الدولية تلزم الأعضاء في المنظمة بإلزامية فرض إجراءات وتدابير ذات طبيعة مختلفة (إدارية وجزائية...)، تتمثل هذه الأخيرة في عقوبات جزائية لمواجهة الاعتداءات الماسة بحقوق المؤلف خاصة القرصنة، ونصت كذلك على إضفاء حماية لبرامج الحاسوب باعتبارها مصنفات أدبية[1]. فهدفها الأساسي إضفاء حماية لحقوق الملكية الفكرية في ظل التطورات التكنولوجية الحالية والمستقبلية، وحماية الملكية الفكرية في الفضاء الرقمي، خاصة

بظهور نوع جديد من المصنفات وهي المصنفات الرقمية، فهذه الأخيرة أسفرت عن إشكالات قانونية بسبب طبيعتها.

وبالتالي فإن هذا النوع من المنظمات الدولية يبرز نشاطها في مجال واحد ومحدد فالاتحاد الدولي للاتصالات هدفه الأساسي حماية أمن المعلومات مقابل ضمان حق الجميع

[1] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة محمد خيضر بسكرة، الجزار، العدد 2، 2015، ص12.

في التواصل، أما منظمة الملكية الفكرية فهدفها الأساسي حماية حقوق الملكية الفكرية بأي صورة كانت تقليدية أو إلكترونية.

المطلب الثاني: دور المنظمات الاقليمية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

للمنظمات الإقليمية دور فعال في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات سواء الأوربية (الفرع الأول)، أو المنظمات العربية والافريقية (الفرع الثاني).

الفرع الأول: دور المنظمات الأوروبية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

للمنظمات الدولية الأوربية العديد من الجهود بهدف مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات منها جهود كل من المجلس الأوربي والاتحاد الأوربي(أولا)، إضافة إلى دور منظمة التعاون الاقتصادي والتنمية OECD (ثانيا).

أولا: دور المجلس الاوربي والاتحاد الأوربي في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

1_ المجلس الأوربي:

بذل المجلس الأوربي[1] جهودًا عديدة لأجل التصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث تم توقيع اتفاقية تحت اشرافه في 28 يناير 1981 تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للمعطيات الشخصية.

[1] مجلس أوروبا Council of Europe هو منظمة دولية يتجسد هدفها المعلن دعم حقوق الإنسان والديمقراطية وسيادة القانون في أوروبا. منشور على الموقع التالي:
https://ar.wikipedia.org/wiki/%D9%85%D8%AC%D9%84%D8%B3_%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D8%A7
تم الإطلاع عليه بتاريخ 11/07/ 2022 على الساعة 10:15.

ولقد أصدر المجلس العديد من القواعد التوجيهية في هذا المجال، ورد فيه ضرورة تجريم العديد من السلوكيات الإجرمية كالغش المعلوماتي وتزوير المعلومات وسرقة الأسرار المخزنة، والتوصل غير المصرح به، كما تضمنت العديد من التدابير التقنية لمنع الدخول غير المرخص به إلى المعلومات المخزنة، مثل حماية كلمات السر والمرور المستخدمة في النهايات الطرفية، وحماية ضوابط التشغيل، وتشفير المعلومات الشخصية، وأسماء المرتبطين بها، ويعتبر أهم عمل قام به المجلس في هذا الشأن هو إشرافه على اتفاقية بودابست التي سبق التفصيل فيها[1].

2_ الاتحاد الأوربي:

اهتمت لجنة الوزراء بالاتحاد الأوربي بالمشاكل المرتبطة بالجرائم المعلوماتية، مشيرة في توصياتها العديدة، إلى تشجيع الدول الأوربية على تبني سياسات مشتركة غايتها تحقيق التفاهم والتعاون الدوليين لمكافحة هذه الجرائم ومن هذه التوصيات:

_ منها ما تتعلق بالبيانات الشخصية في قطاع الشرطة كالتوصية رقم (87) 15، و حماية البيانات الشخصية في مجال الاتصال كالتوصية رقم (95) 4، ومنها المتعلقة بجرائم الكمبيوتر التوصية رقم (89) 9.

_ واصدار التوصية رقم (95) 13 التي تتعلق بمشكلات قانون الإجراءات الجنائية ذات الصلة بتكنولوجيا المعلومات[2]، وبخصوص هذه الأخيرة فإنها صدرت بتاريخ 1995/9/11 وتم فيها حث الدول على مراجعة قوانينها الإجرائية الوطنية لكي تتلاءم مع التطور الحاصل في هذا المجال حيث ورد فيها ما يلي:

[1] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، د.ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص72- 73.

[2] رامي متولي القاضي، عمر سالم، شرح قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 مقارنا بالتشريعات المقارنة والمواثيق الدولية، ط1، مركز الدراسات العربية للنشر والتوزيع، الجيزة، جمهورية مصر العربية، 2020، ص 20.

_ يجب توضيح الإجراءات المتبعة في تفتيش الحواسيب وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء إنتقالها.

_ السماح في قوانين الاجراءات الجزائية الوطنية للجهات المخول لها القيام بإجراء التفتيش من ضبط البرامج والمعطيات وفقا للقواعد والشروط الخاصة بإجراءات التفتيش التقليدية الواردة في قانون الإجراءات الجزائية، مع بيان النظام محل التفتيش والمعطيات المضبوطة

_ امكانية تمديد عملية التفتيش إذا ما كانت الأجهزة متصلة بالنظام محل التفتيش وضبط المعلومات المتضمنة بها وذلك بتوفر شرطين وهما احترام ضمانات التفتيش وأن يكون تمديد التفتيش ضروري.

_ الإبقاء على القواعد التقليدية المتبعة بشأن الوثائق العادية بخصوص المعلومات الرقمية

_ يمكن في حالة الضرورة عند القيام بإجراءات التحقيق تطبيق إجراءات المراقبة والتسجيل مع ضرورة احترام مبدأ السرية وحماية المعلومات التي يقر لها القانون بحماية خاصة

_ إلزامية تعاون عمال المؤسسات التي توفر خدمات الاتصال سواء كانت حكومية أو خاصة مع الجهات المخولة بالتحقيق للقيام بإجراءات المراقبة والتسحيل الالكتروني

_ يتوجب تعديل قانون الاجراءات الجزائية الوطني للدول، وذلك بإصدار أوامر تقضي بضرورة تسليم المعلومات الرقمية بغرض الكشف عن الحقيقة سواء كانت في شكل برامج أو قواعد أم بيانات[1].

_ يجب تمكين جهات التحقيق من أمر أي شخص لديه معلومات خاصة بالدخول إلى نظام المعلومات أو الوصول إلى المعلومات الواردة فيه، واتخاذ التدابير اللازمة لتمكين المحققين من الاطلاع عليها.

[1] شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، الشارقة، الإمارت العربية المتحدة، المجلد 17، العدد1، شوال 1441/ يونيو 2020، ص752.

_ ضرورة تحديث وتوحيد كيفيات التعامل مع الأدلة الإلكترونية في مختلف الدول، مع إمكانية الإبقاء على النصوص التي تخص الأدلة التقليدية وتطبيقها على الأدلة الالكترونية

_ وجوب تأهيل العاملين في مجال العدالة الجنائية من خلال اتباع برامج خاصة لتكوينهم في مجال تكنولوجيا المعلومات، وكذلك إستحداث وحدات خاصة لمكافحة جرائم الكمبيوتر

_ أحيانا تتطلب عملية التحقيق تمديد إجراءاتها إلى أنظمة كومبيوتر متواجدة خارج تلك الدولة، وحتى لا يشكل إجراء التمديد اعتداء على سيادة الدولة والقانون الدولي، وجب سن قواعد إجرائية تنص صراحة على إمكانية القيام بهذا الإجراء، هذا ما يتطلب إبرام اتفاقيات تنظم القواعد التي تحكم هذا الإجراء.

_ وجوب تسريع وتسهيل إجراءات تواصل الجهات المخولة بالتحقيق مع الدول الأجنبية، مع ضرورة سماح هذه الأخيرة بالقيام بإجراءات التفتيش والضبط وإجراء تسجيلات ما يستوجب تطوير الإتفاقيات الدولية بخصوص هذا الشأن[1].

وبناءًا على ما سبق فإن كلا من المجلس الأوربي والاتحاد الأوربي بذل جهود لمواجهة هذه الجرائم والأعمال غير المشروعة المتصلة بتكنولوجيات الإعلام والاتصال من الجانب الموضوعي والإجرائي والتقني، وتجسدت هذه الجهود من خلال القواعد التوجيهة لمجلس أووبا، وتوصيات الاتحاد الأوربي.

[1] شيخة حسين الزهراني، المرجع السابق، ص752- 753.

ثانيا: منظمة التعاون الاقتصادي والتنمية OECD

تعتبر منظمة التعاون الاقتصادي والتنمية[1] السباقة في الاهتمام بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لأكثر من 30 سنة، حيث وضعت مجموعة من الأدلة وقواعد توجيهية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة سنة 1980 مع التوصية للأعضاء بالإلتزام بها[2].

بدأ إهتمامها في بداية الأمر يتجه نحو حماية الخصوصية من التهديد المعلوماتي لها[3]،

عينت منظمة التعاون الاقتصادي والتنمية في عام 1982 لجنة من الخبراء لمناقشة الجرائم المتعلقة بالحواسيب، واقترحت اللجنة عدة اقتراحات، بناء عليها تم التوصية بتعديل قانون العقوبات وبالضبط تعديل النصوص المتعلقة بالجرائم المرتبطة بالحاسوب، وبضرورة تجريم كل الدول الأعضاء السلوكات الإجرامية المرتكبة عمدا في قوانينها الجزائية، مع إلزامية التعاون بين هذه الدول للحد من هذه الأفعال المجرمة، وتضمنت لائحة الجرائم استعمال الحاسوب لأغراض الغش والاحتيال والتزوير، والاعتداءات الواردة على بيانات وبرامج الحاسوب دون إذن، والدخول غير المشروع إلى الأنظمة المعلوماتية والاتصالات السلكية واللاسلكية دون تصريح، والاعتداءات الواقعة على الحقوق التي يتمتع بها أصاحب البرامج المحمية حصرًا دون غيره بقصد استغلالها تجاريا[4].

[1] منظمة التعاون الاقتصادي والتنمية **(Organisation for Economic Co-operation and Development)** واختصارها **(OECD)**، هي منظمة دولية مكونة من مجموعة من البلدان المتقدمة التي تقبل مبادئ الديمقراطية التمثيلية واقتصاد السوق الحر. عبد الإله النوايسية، المرجع السابق، ص48.

[2] مناصرة يوسف، المرجع السابق، ص 273- 274.

[3] بن مكي نجاة، المرجع السابق، ص118.

[4] عبد الإله النوايسية، المرجع السابق، ص 48.

بدأت منظمة التعاون الاقتصادي من سنة 1978 في وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات، وقد تبنت هذه القواعد من قِبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها[1]، وصادقت عليها الدول التالية: الولايات المتحدة الأمريكية، النمسا، نيوزلندا، بلجيكيا، كندا، الدنمارك، المملكة المتحدة، فلندا، فرنسا، ألمانيا، اليونان، اليابان، سويسرا[2]، وأطلق عليها تسمية "المبادئ التوجيهية لمنظمة التعاون الإقتصادي والتنمية (OECD)".

فتعتبر هذه المبادئ التوجيهية الصادرة عن منظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية أول الجهود الدولية المتخصصة في مجال حماية المعطيات الشخصية ونقل المعطيات[3].

وهذه القواعد تتعلق بالأشخاص الطبيعيين فقط وتطبق على القطاعين العام والخاص، وتتعلق أيضا بالبيانات المعالجة آليا أو يدويا، وهذه القواعد ليست إلزامية وإنما تمثل مجرد إرشادات وتوصيات[4]، إلا أنها تحث الدول الأعضاء على إقرار نوع من التوازن في هذا المجال[5].

[1] مروة زين العابدين صالح، مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الدولي الإتفاقي والقانون الوطني، ط1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، 2016، ص 297.

[2] خواثرة سامية، المبادئ الأساسية لحماية البيانات الشخصية بين الجهود الدولية والتشريع الجزائري، مجلة الدراسات القانونية والبحوث الانسانية، كلية العلوم الانسانية والاجتماعية، جامعة العربي التبسي، تبسة، المجلد 07، العدد03، ماي 2022، ص318.

[3] مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر الواد، الجزائر، المجلد10، العدد01، أفريل 2019، ص1306.

[4] مروة زين العابدين صالح، المرجع نفسه، ص 297- 298.

[5] كمال بوبعاية، مبروك لمشونشي، الحماية القانونية الدولية للمعطيات الشخصية في البيئة الافتراضية، مجلة الدراسات القانونية والسياسية، جامعة طاهر مولاي سعيدة، الجزائر، المجلد 07، العدد01، جانفي 2021، ص75.

أ_ المبادئ التوجيهية الصادرة عن منظمة التعاون الاقتصادي والتنمية بشأن حماية الخصوصية:

تتضمن هذه التوجيهات المبادئ الثمانية الرئيسية لحماية الخصوصية أو الحق في حماية البيانات الخاصة، وهذه المبادئ هي:

_ مبدأ تحديد حصر عمليات جمع البيانات والإقتصار على طبيعة البيانات الشخصية وتحديدها Collection Limitation Principle: ويطلق عليه كذلك تسمية **(مبدأ تقييد التحصيل)**، ينص هذا المبدأ على وجوب فرض قيود (حدود) على عملية جميع البيانات الشخصية، ووجوب أن تكون عملية الحصول عليها بطريقة مشروعة وعادلة، وبعد الحصول على موافقة صاحب البيانات[1].

_ مبدأ جودة البيانات Data Quality Principle: حيث يجب أن تكون البيانات الشخصية مرتبطة بالأغراض التي سيتم استخدامها من أجلها، ويجب أن تكون دقيقة وكاملة ومحدثة بالقدر اللازم لتلك الأغراض[2].

_ مبدأ تحديد الغرض Purpose Specification Principle: يجب تحديد الأغراض التي يتم جمع البيانات الشخصية من أجلها في موعد لا يتجاوز وقت جمع البيانات والاستخدام اللاحق يقتصر على تحقيق تلك الأغراض أو غيرها من الأغراض التي لا تتعارض مع تلك الأغراض وكما هو محدد في كل مناسبة من حالات التغيير الغرض[3].

[1]" Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject". OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, Legal Instruments, 2022.

[2] " Data Quality Principle : Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up to date."
OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[3] " Purpose Specification Principle : The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

_ مبدأ حصر الاستخدام بالغرض المحدد Use Limitation Principle: ويطلق عليه كذلك تسمية مبدأ حدود الاستخدام أو مبدأ تقييد الاستخدام، والذي ورد فيه أنه يجب عدم الكشف عن البيانات الشخصية أو إتاحتها أو استخدامها لأغراض أخرى غير تلك الأغراض المحددة باستثناء:

- موافقة صاحب البيانات
- أو بموجب سلطة القانون[1].

_ مبدأ توفير وسائل حماية وأمن المعلومات Security Safeguards Principle: **ويصطلح عليه أيضا** مبدأ الضمانات الأمنية حيث يجب حماية البيانات الشخصية بضمانات توفر الحماية الأمنية المعقولة ضد مخاطر مثل فقدان البيانات أو الوصول غير المصرح به أو إتلافها أو استخدامها أو تعديلها دون تصريح أو الكشف عنها دون إذن[2].

_ مبدأ العلانية Openness Principle: يجب أن تكون هناك سياسة عامة للعلنية حول التطورات والممارسات والسياسات المتعلقة بالبيانات الشخصية. يجب أن تكون الوسائل متاحة بسهولة لإثبات وجود وطبيعة البيانات الشخصية، والأغراض الرئيسية لاستخدامها، بالإضافة إلى الهوية والإقامة المعتادة لمراقب البيانات[3].

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[1] " Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law."
OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[2] " Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data".
OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[3] " Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller".

_ مبدأ المشاركة الفردية Individual Participation Principle: يجب أن يكون للأفراد الحق في الحصول من مراقب البيانات، أو غيره على تأكيد ما إذا كانت البيانات متعلقة به لدى المراقب البيانات، وإذا كانت البيانات المتعلقة بهم موجودة لابد من بها إبلاغهم بهما في غضون فترة زمنية معقولة، وفي هذين الحالتين يجب تسبيب رفض الطلب المقدم، ومع ذلك يبقى الأفراد لديهم الحق في الطعن، وكذلك لديهم الحق في الاعتراض على البيانات المتعلقة بهم، وإذا تم قبول هذا الإعتراض يمكنهم يتم محو البيانات أو تصحيحها أو تكملتها أو تعديلها. وإن كانت هذه البيانات موجودة يجب لا تكون مفرطة أي يتم جمعها بطريقة معقولة، وأن تكون في شكل يمكن (يسهل) فهمه بسهولة[1].

_ مبدأ المساءلة Accountability Principle: يجب أن يكون مراقب البيانات مسؤولاً عن الامتثال للتدابير التي تؤدي إلى تنفيذ المبادئ المذكورة أعلاه[2].

والسؤال الذي يُطرح في هذا الصدد يتمثل في مدى إلزامية الأدلة والقواعد التوجيهية الصادرة عن هذه المنظمة؟ وكإجابة على هذا التساؤل منظمة التعاون والتنمية الاقتصادية على الرغم من أن لها سلطة اتخاذ القرارات، إلا أنها لا تملي قواعد ملزمة، والأساس في هذه المنظمة هو ميدان الفكر وتبادل الآراء وجهات النظر وليس القرار الملزم، فالالتزام الذي بين

[1] Individual Participation Principle
Individuals should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
b) to have communicated to them, data relating to them
i. within a reasonable time;
ii. at a charge, if any, that is not excessive;
iii. in a reasonable manner; and
iv. in a form that is readily intelligible to them;
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended."
OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

[2] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

للاطلاع على الوثيقة منشورة على الموقع التالي: file:///C:/Users/user/Downloads/OECD-LEGAL-0188-en.pdf

الدول هو التزام سياسي لأن كل دولة لها مصلحة في القرارات التي تنفذها الدول الأخرى، وهذا يؤدي إلى إنشاء ضغط قوي وفعال لإحترام كل الالتزامات، ويعتبر كل من الإجماع والضغط مبدأين أساسيين في المنظمة[1]، وبالتالي فالأدلة والقواعد التوجيهية الصادرة عن هذه المنظمة غير ملزمة بالنسبة للدول الأعضاء.

وما يجدر الاشارة إليه في هذا الصدد هو أن هذه المبادئ التوجيهية المقررة لدى منظمة التعاون الاقتصادي والتنمية ودليل مجلس أوروبا، مضمونها يتطابق مع مضمون المبادئ التوجيهية لتنظيم الملفات المحوسبة التي تحتوي على بيانات شخصية من حيث الإلزامية فهي مبادئ غير ملزمة لأنها تمثلت في توصيات للدول الأعضاء لأجل النص عليها في تشريعاتها الوطنية ليس لديها أي قوة إلزامية[2]، ولا يترتب على عدم النص عليها جزاء.

الفرع الثاني: دور جامعة الدول العربية باعتبارها منظمة عربية

إن من أهم الأهداف لجامعة الدول العربية تنسيق وتعزيز التعاون بين الدول الأعضاء في مكافحة الإجرام بمختلف أشكاله بما فيه الإجرام المستحدث والذي يشكل أبرز نموذج له الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ومن خلال هذا الفرع سنتطرق إلى دور جامعة الدول العربية باعتبارها منظمة عربية في مكافحة الجرائم السابقة الذكر من خلال مجلس وزراء العدل العرب (أولا)، جامعة نايف العربية للعلوم الأمنية (ثانيا).

[1] عطابة زهية، المساهمة التشريعية لمنظمة التعاون والتنمية الاقتصادية في التنمية الاقتصادية، دفاتر البحوث العلمية، المركز الجامعي تيبازة، الجزائر، المجلد 5، العدد 11، ديسمبر 2017، ص432.

[2] بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي سعيدة، الجزائر، العدد6، جوان 2016، ص 281.

أولا: مجلس وزراء العدل العرب

لمجلس وزراء العدل العرب دور مهمًا لا يستهان به باعتباره الجهاز المعني بتحقيق التعاون الأمني ومكافحة الجريمة المنظمة بأشكالها المختلفة، بما فيها الجرائم السيبرانية بصفة عامة وكذلك الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة كون الوطن العربي يشهد انتشار متزايد لهذه الجرائم، وهذا مرده قصور التشريعات العربية وعدم قدرتها على مواكبة التطور التقني والتكنولوجي الذي يشهده المجتمع، إضافة إلى عدم إحكام الرقابة على الحدود العربية، هذا ما يستدعي بالضرورة توحيد الجهود العربية باعتماد أساليب واستراتيجيات موحدة لمكافحة هذا النوع من الإجرام من قبل مجلس الوزراء العرب باعتباره كما قلنا سابقا الجهاز المسؤول عن تحقيق وتنفيذ التعاون الأمني في الوطن العربي[1].

فعلى الصعيد العربي تم بذل جهود حقيقية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والمتصلة منها بتكنولوجيا المعلومات – إلا أن المكافحة التشريعية لهذا النوع من الجرائم جاءت متأخرة مقارنة بمواجهة الدول الأخرى لها –

إعتمد المؤتمر السادس للجمعية المصرية للقانون الجنائي في مجال الجرائم الإلكترونية سنة 1993 عدة توصيات تتعلق بتحديد مختلف أشكال السلوك الإجرامي في الجرائم المعلوماتية وتحديدها، وأصدرت منظمة جامعة الدول العربية وبالضبط المنظمة العربية للتنمية الإدارية التابعة لها العديد من التوصيات في ندوة الدليل الرقمي التي عقدت في القاهرة في الفترة من 5 إلى 8 مارس 2006، وركزت التوصيات جلها على جانبين وهما الجانب الإجرائي والجانب التدريبي في مجال الجرائم المتعلقة بتكنولوجيا المعلومات[2].

[1] محمد الصغير سليني، المرجع السابق، ص242.

[2] عبد الإله النوايسية، المرجع السابق، ص53.

وأولت الجامعة العربية اهتماما بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وذلك من خلال الأمانة العامة لمجلس وزراء الداخلية العرب، حيث تم تخصيص الاجتماع الخامس للجنة المتخصصة بالجرائم المستجدة لجرائم الانترنت.

بالإضافة إلى عقد اجتماع فريق عمل مخصص لدراسة الجرائم المرتكبة بواسطة الحواسيب وشبكات الانترنت (تونس: 23- 2000/3/24 م)، وكذلك تخصيص الاجتماع الثامن للجنة المتخصصة بالجرائم المستجدة (تونس: 15-5/16/ 2000م) وبالضبط لموضوع جرائم نظم المعلومات وسبل مكافحتها، وتطبيقا للتوصية الصادرة عن هذا الاجتماع أعدت الأمانة العامة نموذجًا موحد لجهاز متخصص في مكافحة جرائم نظم معالجة المعطيات وتم تعميمه عام 2002 على جميع الدول الأعضاء للاستفادة منه. بالإضافة إلى إعداد دراسة حول الإجراءات والتدابير الرامية إلى منع ومكافحة الجرائم المرتكبة بواسطة الحاسبات الإلكترونية وشبكات الانترنت عرضت على الدورة رقم 20 لمجلس وزراء الداخلية العرب (تونس: 13-1/14/ 2013) وتم تعميمها كذلك على الدول الأعضاء للاستفادة منها[1].

وقامت بالعديد من المؤتمرات منها:

_ المؤتمر العربي السادس عشر لرؤساء أجهزة المباحث والأدلة الجنائية: انعقد بتونس بتاريخ 2017/5/15، ناقش هذا المؤتمر عدة مواضيع من أهما موضوع ضبط الأدلة الإلكترونية وكيفيات التعامل معها، ومختلف المستجدات المتعلقة بالجريمة الإلكترونية، ودرس هذا المؤتمر مسألة تكوين فريق خبراء من المختصين في الجرائم الإلكترونية في مختلف مجالاتها سواء كانت أمنية أو قانونية أو تقنية[2].

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص29.

[2] الموقع الرسمي لمجلس وزراء الداخلية العرب، متوفر على الرابط التالي:
https://www.aim-council.org/news/secretariat-news/1016/
تم الاطلاع عليه بتاريخ: 03/02/ 2023 على الساعة 10:19.

_ المؤتمر العربي العاشر لرؤساء مؤسسات التدريب والتأهيل الأمني: الذي عقد بتاريخ 18جويلية سنة 2017، والذي من أهم التوصيات الصادرة عنه: تدريب رجال الشرطة وفق برامج ومناهج مستحدثة بغرض مكافحة جل أشكال الظواهر الاجرامية التقليدية والمستجدة، والاهتمام بشكل خاص بتدريب المدربين في هذا المجال، كما أوصى كذلك هذا المؤتمر الدول الأعضاء باستخدام أساليب تدريب حديثة تتماشى مع نوعية وخصوصية التحديات الأمنية المستجدة[1].

ثانيا: جامعة نايف العربية للعلوم الأمنية

تم تأسيس جامعة نايف للعلوم الأمنية عام 1980، وذلك بموجب قرار صادر عن مجلس وزراء الخارجية العرب، تتخصص في مجال البحث العلمي والتدريب في مجالات منع الجريمة والعدالة الجنائية، ويشارك جميع الدول الأعضاء في جامعة الدول العربية في أنشطتها وبرامجها[2]، وقعت الأكاديمية اتفاقية تعاون مع برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية فيينا 1986، وتحمل هذه الجامعة صفة مراقب لدى المجلس الاقتصادي والاجتماعي التابع لمنظمة الأمم المتحدة، وتعتبر منظمة إقليمية حسب قرار المجلس رقم 165 لعام 1989[3].

احتضنت يومي 18 و19 ماي 2022 اللقاء الأول لفريق الخبراء العرب المعني بمواجهة جرائم تقنية المعلومات، وتم التأكيد من خلاله على ضرورة توحيد الجهود العربية ودعم التعاون المشترك لمكافحة الجرائم المتعلقة بتقنية المعلومات، حيث ساهم اهتمام

[1] الموقع الرسمي لمجلس وزراء الداخلية العرب، متوفر على الرابط التالي:
https://www.aim-council.org/news/secretariat-news/1029/
تم الاطلاع عليه بتاريخ: 02/03/ 2023 على الساعة 10:45.

[2] ملاوي قدور، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة ماجستير القانون الجنائي الدولي، كلية الحقوق والعلوم السياسية جامعة البليدة 2، الجزائر، 2017، ص129.

[3] ملاوي قدور، المرجع نفسه، ص129.

الجامعة بالجرائم السيبرانية وأمن المعلومات في النجاح الذي حققه مركز الجرائم السيبرانية والأدلة الرقمية التابع لها بالرغم من حداثته[1].

1_ مركز الجرائم السيبرانية والأدلة الرقمية:

تم تأسيس المركز سنة 2021[2]، حيث يهدف إلى تدريب وتكوين المتخصصين في جمع الأدلة الرقمية دون إتلافها وكيفيات التعامل مع هذا النوع الجديد من الأدلة وتحليلها، ومن ثم التقارير التقنية والفنية، ويُشرف هذا المركز على التدريب في مجال الجرائم السيبرانية في 4 تخصصات، جميعها تتعلق بالأدلة الرقمية وهي:

- الأدلة الجنائية الرقمية للوسائط المتعددة
- الأدلة الجنائية الرقمية للشبكات
- الأدلة الجنائية الرقمية للحاسب
- الأدلة الجنائية الرقمية للجوال وطائرات الدرونز[3].

---

[1] محمد بن علي كومان، أخبار مجلس وزراء الداخلية العرب، فريق من الخبراء العرب يعقدون لقاءهم الأول في جامعة نايف لمواجهة الجرائم الالكترونية، مجلة الأمن والحياة، جامعة نايف العربية تدعو لتبني إستراتيجية للحد من حرائق الغابات، العدد 442، أبريل– يونيو 2022، ص10.

متوفر على الرابط التالي:

https://amn_mag.nauss.edu.sa/versions/442/mobile/index.html

تم الاطلاع عليه بتاريخ: 03/10/ 2023 على الساعة08:45.

[2] يعتبر المرجع العربي الأول في تمكين الكفاءات العربية في مجال الجرائم السيبرانية والأدلة الرقمية.

أخبار جامعة نايف، دراسة لجامعة نايف: 137 ألف عربي يزور مواقع الاحتيال المالي يوميا، مجلة الأمن والحياة، العدد 441، يناير– مارس 2022، ص 56.

الموقع الرسمي لجامعة نايف العربية للعلوم الأمنية، متوفر على الرابط التالي:

https://amn_mag.nauss.edu.sa/versions/441/mobile/index.html

تم الاطلاع عليه بتاريخ 2023/03/29 على الساعة 16:30.

[3] الموقع الرسمي لجامعة نايف العربية للعلوم الأمنية، متوفر على الرابط التالي:

https://nauss.edu.sa/ar-sa/colleges-and-centers/cyber-crime-center-and-digital-evidence/Pages/about-center.aspx

تم الاطلاع عليه بتاريخ 2023/03/29 على الساعة 16:49.

وبالتالي فهذا المركز يهتم بعلم الأدلة الجنائية الرقمية، والذي يصطلح عليه علم التحليل الجنائي الرقمي، وهذا بغرض الكشف عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وتحديد مرتكبيها بدقة، ولغرض التصدي لتحديات إثباتها وتعقيداتها.

2_ المنظمة العربية لتكنولوجيا الاتصال والمعلومات (AICTO):

هي منظمة متخصصة منبثقة عن جامعة الدول العربية[1]، هي منظمة حكومية عربية متخصصة، مقرها الجمهورية التونسية، وتعمل تحت رعاية جامعة الدول العربية. تهدف إلى المساهمة في تطوير تكنولوجيات المعلومات والاتصال في الدول العربية وتوفير الآليات اللازمة لدعم التعاون والتكامل في هذا الشأن بين أعضاء المنظمة ووضع سياسات واستراتيجيات مشتركة وتطوير هذه السياسات، بغرض لنشر الوصول العادل والمستدام إلى التكنولوجيا وتكييفها لخدمة أهداف التنمية الاقتصادية والتقدم الإجتماعي المنطقة العربية، قامت بدراسات متعددة منها: "الانتقال للنسخة السادسة من برتوكول الانترنت، الرؤية العربية للأمن السيبراني، الاستراتيجية العربية للأمن السيبراني 2027/2023"[2].

---

[1] نشأت " المنظمة العربية لتكنولوجيات الاتصال والمعلومات"، والتي تعتبر إحدى المنظمات العربية المتخصصة المنبثقة عن جامعة الدول العربية، سنة 2001 بموجب قرار مجلس جامعة الدول العربية في اجتماعه (116) بتاريخ 10 /09/ 2001 و قرار المجلس الاقتصادي والاجتماعي لجامعة الدول العربية رقم 1436 الصادر بتاريخ 13 /02/ 2002 في دورته (69).

دخلت إتفاقية انشاءها حيز النفاذ ابتداء من تاريخ 17 /09/ 2005، و تم تعديلها سنة 2018 بموجب قرار المجلس الاقتصادي والاجتماعي لجامعة الدول العربية رقم 2194 – في دورتها العادية (102) الصادر في 06 /09/ 2018.

متوفر على الرابط التالي:

http://www.aicto.org/ar/%d8%b9%d9%86-%d8%a7%d9%84%d9%85%d9%86%d8%b8%d9%85%d8%a9/%d9%84%d9%85%d8%ad%d8%a9-%d8%b9%d9%86-%d8%a7%d9%84%d9%85%d9%86%d8%b8%d9%85%d8%a9/%d8%a7%d9%84%d8%a5%d9%86%d8%b4%d8%a7%d8%a1/

تم الاطلاع عليه بتاريخ 2023/03/29 على الساعة 18:00.

[2] الموقع الرسمي للمنظمة العربية لتكنولوجيا الاتصال والمعلومات، متوفر على الرابط التالي:

وما يلاحظ أن مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى العربي لاقى اهتماما كبيرا من جامعة الدول العربية، هذا ما ساهم في بلورة معالم السياسة الجنائية لمكافحة هذا النوع من الجرائم على المستوى الاقليمي.

المبحث الثاني: مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في التشريعات الدولية

اتجهت الإرادة الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وتجسيدا لهذه الرغبة، ونتيجة للجهود الدولية المبذولة ظهرت العديد من التشريعات الدولية على المستوى العالمي وعلى الإقليمي، بغرض التصدي لهذه الجرائم المستحدثة العابرة للحدود الوطنية، حيث لا تستطيع الدولة بمنأى عن بقية الدول أن تجابهه بمفردها، لذا ظهرت العديد من الصكوك والمواثيق الدولية والاتفاقيات، ففي البداية برزت الاتفاقيات الدولية المكافحة للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بكل أنواعها التي يكون فيها نظام المعالجة الآلية للمعطيات محلا للجريمة، والتي يكون فيها وسيلة لإرتكاب الجريمة، ثم بدأت تتجسد في الظهور التشريعات الدولية المتعلقة بحماية المعطيات الشخصية على المستوى الدولي.

لذا من خلال هذا المبحث سنتطرق إلى التشريعات الدولية العامة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، التشريعات الدولية المتعلقة بحماية المعطيات الشخصية (المطلب الثاني).

---

http://www.aicto.org/ar/%d8%b9%d9%86-%d8%a7%d9%84%d9%85%d9%86%d8%b8%d9%85%d8%a9/%d9%84%d9%85%d8%ad%d8%a9-%d8%b9%d9%86-%d8%a7%d9%84%d9%85%d9%86%d8%b8%d9%85%d8%a9/%d9%85%d9%86-%d9%86%d8%ad%d9%86-%d8%9f/

تم الاطلاع عليه بتاريخ 2023/03/29 على الساعة 18:10.

المطلب الأول: التشريعات الدولية العامة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تنوعت التشريعات الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، الشاملة لكل أنواع هذه الجرائم دون تخصيص هذه التشريعات لمكافحة جريمة من هذه الجرائم على وجه التخصيص سواء واقعة على النظام في حد ذاته أو معطياته، أو واقعة بواسطته أو يُسهل هو إرتكابها عن طريق الأنترنت.

فتجلت التشريعات الدولية على المستوى الإقليمي، ورغم خطورة هذه الجرائم إلا أنه لا توجد إتفاقية على المستوى العالمي خاصة بمكافحتها وإنما وجدت فقط إتفاقيات إقليمية المنشأ في هذا الشأن.

واستنادًا لما سبق ذكره قسمنا هذا المطلب إلى تشريعات مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الأوربي (الفرع الأول)، تشريعات مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى العربي (الفرع الثاني).

الفرع الأول: تشريعات مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الأوربي

يعتبر التعاون الدولي الآلية المثلى لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، كون الدول مهما كانت متقدمة فإنها لا يمكنها بمفردها مجابهة هذه الجرائم مهما وضعت لها من تشريعات وعقوبات لغرض الحد منها، لأنها لا تستطيع بمفردها تجاوز تحدي عبورها للحدود الوطنية، الذي لا يوقفه عائق جغرافي لأن محلها البيئة الافتراضية، لذلك فغالبية الدول تفضل الانضمام إلى الاتفاقيات الدولية المبرمة لأجل مكافحة هذه الجرائم، ومنها الدول الأوربية التي رغم تقدمها ولكن لا يمكنها مواجهتها بمفردها، دون وجود

تعاون دولي[1]، لذا تم إبرام إتفاقية على المستوى الأوربي لأجل مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات. والتي برز لها دور فعال في مكافحة هذه الجرائم، هذا ما سنتطرق إليه من خلال هذا الفرع.

أولا: الاتفاقية الأوربية المتعلقة بالجريمة المعلوماتية

تسمى كذلك بإتفاقية بودابست، أو الاتفاقية رقم 185.

بغرض مواجهة الارتفاع المستمر لجرائم الكمبيوتر، قررت الدول المتمدنة وضع تشريعات خاصة لمكافحة جرائم الكمبيوتر التي تعتبر ظاهرة جديدة في علم الإجرام وتشمل هذه الدول الولايات المتحدة وفرنسا وبقية دول الاتحاد الأوروبي، الذي وضع اتفاقية بشأن جرائم الكمبيوتر في عام 2001م، أوصت هذه الأخيرة بأن تتخذ الدول الأعضاء جميع الإجراءات التشريعية اللازمة وغيرها من الإجراءات لجعل الدخول غير المشروع إلى جميع أنظمة الكمبيوتر أو أي من أجزائها جريمة جنائية بموجب القانون الوطني، كما أوصت هذه الاتفاقية بمجموعة من المبادئ العامة المتعلقة بالتعاون الدولي في المسائل الجنائية، كما حددت مختلف الإجراءات المتعلقة بطلبات المساعدة المتبادلة بين الدول في حالة عدم وجود اتفاقيات دولية، اعتمد الاتحاد الأوروبي التشريع على غرار اتفاقية بودابست. حيث يهدف واضعو هذه الاتفاقية إلى تشجيع الدول الأعضاء على مواءمة التشريعات الوطنية مع أحكام الاتفاقية ونصوصها، بالإضافة إلى الحاجة إلى استكمال الأدوات القانونية لهذه البلدان في جانب الإجراءات، وذلك من أجل تحسين القدرة المدعين العامين على جمع الأدلة[2].

[1] بن مكي نجاة، المرجع السابق، ص 122- 123 .

[2] ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، منشور على الرابط التالي: https://www.ahewar.org/debat/show.art.asp?aid=571423 تم الاطلاع عليه بتاريخ: 2022/05/31 على الساعة 15:15.

تم تجسيد مشروع هذه الإتفاقية الذي سبق طرحه في المحفل الأوربي منذ فترة طويلة بغرض وضع أساس قانوني للتشريعات الموضوعية والإجرائية وركيزة للتعاون الدولي لمكافحة الجرائم المعلوماتية[1].

فتعتبر أول معاهدة اتفاقية دولية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ساهمت في بلورة التعاون والتضامن الدولي في مكافحتها ومحاولة الحد منها، لاسيما بعد التطور الهائل الذي شهدته هذه الجرائم ووصولها إلى حد خطير أصبح يهدد الأشخاص والممتلكات[2]، حيث أنه بتاريخ 23 نوفمبر لسنة 2001 في عاصمة المجر وبالضبط في مدينة بودابست BUDABEST[3] وقعت على هذه الاتفاقية (30) دولة، منها (26) دولة أوروبية وكندا واليابان وجنوب إفريقيا والولايات المتحدة الإمريكية، وبالرغم من أن هذه المعاهدة تعتبر أصلها أوربية المنشأة، إلا أنها إتفاقية ذات طابع دولي، وهي مفتوحة لمختلف الدول لطلب الإنضمام إليها، واستغرقت المباحثات والمفاوضات بين الدول الموقعة عليها أربع سنوات إلى غاية أن تم التوصل إلى صيغتها النهائية المعروفة، ضف إلى ذلك تم الإتفاق من خلالها على أهمية التعاون والتضامن الدولي في مجال مكافحة هذه الجرائم[4]. ويعتبر التوقيع على معاهدة بودابست أول خطوة لتكوين تضامن دولي مكافح للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، والتي يُساء استخدام الانترنت فيها، فالهدف الأساسي من هذه الاتفاقية هو توحيد الجهود الدولية[5].

وافتتحت هذه الاتفاقية باب التوقيع منذ تاريخ صدورها حيث بتاريخ 30 سبتمبر 2004 وصل عدد الدول الموقعت عليها إلى 30 دولة موقعة من مجلس أوروبا، و4 دول غير أوروبية كما سبق ذكره، وبتاريخ 2010/02/01 تم التصديق عليها من طرف 25 دولة من

[1] مناصرة يوسف، المرجع السابق، ص 286.

[2] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 21.

[3] مناصرة يوسف، المرجع نفسه، ص 286.

[4] رامي متولي القاضي، عمر سالم، المرجع نفسه، ص22.

[5] بن مكي نجاة، المرجع السابق، ص 122.

الدول 47 الأعضاء في المجلس الأوربي، ثم أصبح عدد الأعضاء المصادقة (56) دولة أما الموقعة دون تصديق (4) دول في سنة 2018، وبخصوص الدول الغير أعضاء في مجلس أوروبا أغلبها وقعت عليها دون المصادقة مثل كندا وكوستاريكا واليابان والميكسيك وجنوب إفريقيا وموريس وبنما وجمهورية الدومينيك والسنغال وسيريلانكا وكونغا، اما الولايات المتحدة الإمريكية فقد صادقت عليها رغم عدم إنتمائها للدول الأعضاء في مجلس أوروبا وهذا لأهمية هذه الإتفاقية[1].

ووصل عدد الدول الأطراف فيها عام 2022 إلى 69 دولة، حيث أصبح عدد الأعضاء المصادقة (67) دولة، أما الموقعة دون تصديق (2) دول إلى غاية الآن سنة 2022[2].

وتعتبر أحكام هذه الاتفاقية ملزمة للدول الأطراف، سواء ما تعلق منها بالجانب الموضوعي، أو الأحكام الإجرائية من تعاون دولي إجرائي[3].

وتتكون هذه الاتفاقية من 48 مادة مقسمة إلى أربعة (4) فصول، قُسِمت هذه الإتفاقية إلى 48 مادة، وورد في هذه الإتفاقية الجرائم الأكثر انتشارا في العالم، كالإرهاب الإلكتروني، عمليات تزوير بطاقة الإئتمان ودعارة الأطفال، كما حددت إجراءات التحقيق في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، واتفقت الدول الموقعة على محاربتها، والموازنة بين المقترحات المقدمة من أجهزة الشرطة، والمخاوف التي أعربت عنها منظمات حقوق الإنسان، ومقدمي خدمات الإنترنت، حيث أن منظمات حقوق الإنسان كانت قلقة من

[1] مناصرة يوسف، المرجع السابق، ص 300- 301.

[2] the Budapest Convention Chart of Signatures and Ratifications, available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 accessed : Septmber 02, 2022 At13:10.

[3] Cesare Parodi, Valentina Sellaroli, DIRITTO PENALE DE LL'INFORMATICA, REATI DELLA RETE E SULLA RETE, Giuffré Francis lefebvre, milano, 2020, P713.

أن هذه الاتفاقية ستحد من حرية الأفراد وأن الرقابة ستؤدي إلى انتهاك حقوق مستخدمي الإنترنت[1].

فهذه الاتفاقية جسدت ولأول مرة إطارا لتحديد قائمة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وأنواعها وطوائفها، فلحد الآن وبالرغم من وجود الكثير من الجهود التشريعية وكذلك الاجراءات الإقليمية والدولية، طيلت ثلاثين سنة الماضية إلا أنه لم تكن هناك رؤية عالمية كاملة وواضحة، وإطار يحدد قائمة الأفعال المُجَرّمة أو يُبين معايير التقسيم، لذلك فإن أهم ما ورد في هذه الاتفاقية أنها وضعت إطار لتقسيم وللتحديد بخصوص القواعد الموضوعية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والإنترنت[2].

1_ الجرائم التي تضمنتها إتفاقية بودابست:

إعتمدت هذه الاتفاقية معيار يقوم على فكرة دور جهاز الكمبيوتر في الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث أنها قسمت الجرائم إلى أربعة (4) أقسام[3].

أ_ الطائفة الأولى: تمثلت في الجرائم التي تستهدف أمن المعلومات، أو ما يطلق عليها الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية[4]، والتي نصت عليها كل من المادة 2، 3، 4،5، 6 على التوالي من الإتفاقية، وهي كالتالي:

_ جريمة النفاذ غير القانوني: نصت على هذه الجريمة المادة 2 من إتفاقية بودابست. يتمثل ركنها المادي النفاذ غير القانوني حيث يكون هذا النفاذ أو الدخول غير مرخص به من طرف مالك نظام المعالجة الآلية للمعطيات، أو من له حق على هذا النظام أو جزء

[1] شيخه حسين الزهراني، المرجع السابق، ص 754-755.

[2] مروة زين العابدين صالح، المرجع السابق، ص 439.

[3] مروة زين العابدين صالح، المرجع نفسه، ص 439.

[4] Convention sur la cybercriminalité, Série des traités européens - n° 185, Conseil de l' Europe, Budapest, 23.XI.2001.

منه، وما يجدر التنويه إليه أنه حتى تكون هناك حماية جنائية لنظام المعالجة لابد أن يكون غير مفتوح للجمهور، وأن لا يوفر نفاذ مجاني.

وغالبا يكون النفاذ غير القانوني يتخذ أحد هذه الأشكال إما في صورة " قرصنة " أو " كسر" أو " إختراق الكمبيوتر"، ويمكن أن يكون النفاذ إلى نظام المعالجة الآلية للمعطيات كليًا أو جزئيًا. وقد يأخذ شكل هذا النفاذ صورة نفاذ إلى نظام معالجة لجهاز آخر عن بعد أو على مسافة قصيرة، أو عبر روابط لاسلكية[1]. ويتمثل الركن المعنوي في هذه الجريمة في نية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى[2].

ـ جريمة الإعتراض غير المشروع أو الاعتراض غير القانوني: يكون فعل الاعتراض غير المشروع أو الاعتراض غير القانوني بالوسائل التقنية، وتشمل هذه الوسائل الأجهزة التقنية المثبتة على خطوط النقل وأجهزة جمع وتسجيل الاتصالات اللاسلكية، ويمكن أن يتم هذا الاعتراض أيضًا من خلال برامج مخصصة للاعتراض، وكلمات المرور والرموز، أو من خلال التنصت فيتم الاطلاع على مضمون الاتصالات ورصدها إلكترونيا، ويكون هذا التصنت بطريقتين الأولى مباشرة، من خلال الشراء المباشر لمحتوى البيانات والولوج إلى نظام المعالجة الآلية للكمبيوتر واستخدامه، والثانية تكون بشكل غير مباشر من خلال استخدام أجهزة التنصت الالكترونية على المكالمات الهاتفية[3]. وهذه الجريمة عمدية يجب أن يرتكب الإعتراض غير المشروع عمدا، وبدون حق، وقد ورد ذكر هذه الحالات على سبيل المثال لا الحصر في التقرير التفسيري لاتفاقية بودابست وتكون هذه الحالات إذا كان فعل

[1] أنظر المادة 2 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مجلس أوربا، سلسلة المعاهدات الأوروبية رقم 185، بودابست، المجر، 23 نوفمبر 2001.

[2] Art 02 de la Convention sur la cybercriminalité.

[3] أنظر المادة 3 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

الاعتراض حق من حقوق المعترض، أو بناءًا على تعليمات أو إذن أو كان مخول قانونا للمصلحة العامة، أو لكشف جرائم[1].

ـ جريمة الإعتداء على سلامة البيانات: هذه الجريمة نصت عليها المادة 4 من الاتفاقية، والتي كانت تهدف إلى حماية بيانات الكمبيوتر وبرامجه، يتمثل السلوك المادي لهذه الجريمة في الإضرار، أو المحو، أو تعطيل، أو إتلاف، أو طمس لبيانات الحاسب[2]. وتعتبر هذه الجريمة عمدية، ترتكب فيها الأفعال المذكورة سابقا عمدا وبدون حق. بمعنى أنه إذا تمت تلك الأفعال التي ذكرناها سابقا بوجه حق، حتى لو كانت عمدا فإنه لا يعاقب مرتكبها[3].

ـ جريمة التدخل في النظام (الإعتداء على سلامة النظام): وهذه الجريمة منصوص عليها في المادة 5 من الاتفاقية، وتجرم هذه المادة العرقلة والتي تعتبر بمثابة عائق وتتمثل في الإجراءات التي تعرقل حسن سير عمل نظام الكمبيوتر، ويجب أن يتم هذا العائق عن طريق إدخال بيانات الكمبيوتر أو نقلها أو إتلافها أو حذفها أو تعديلها أو إتلافها. ويشترط في هذه العرقلة أن تكون غير قانونية وجسيمة وخطيرة وبدون وجه حق[4]. وتكون هذه الجريمة عمدية، حيث يجب أن يكون لدى الجاني المعلوماتي نية عرقلة نظام المعالجة بشكل جسيم[5].

ـ جريمة إساءة إستخدام الأجهزة (أجهزة الحاسب): تعتبر هذه الجريمة منفصلة عن الجرائم المذكورة في هذه الاتفاقية التي ذكرناها سابقا والمنصوص عليها في المواد من 2 إلى5.

---

[1] أنظر المادة 3 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[2] هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقًا عليها، ط1، دار النهضة العربية، القاهرة، 2007، ص 75-76.

[3] أنظر المادة 4 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[4] أنظر المادة 5 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[5] أنظر المادة 5 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

يتمثل الركن المادي في إنتاج أو بيع أو شراء للاستخدام أو الاستيراد أو التوزيع أو إتاحة بأي طريقة أخرى لأي برنامج كمبيوتر مصمم أو معدة خصيصًا لغرض ارتكاب أي من الجرائم المنصوص عليها في المواد التي ذكرناها سابقا (من م 2 إلى م 5 من هذه الاتفاقية). ومثال هذه البرامج برامج الفيروسات أو البرامج المصممة أو المكيفة للوصول إلى النفاذ إلى أنظمة المعالجة الآلية[1]، وهذه الجريمة هي جريمة عمدية.

وبالتالي فالفئة الأولى من جرائم هذه الاتفاقية تتمثل في الجرائم التي يتخذ فيها نظام المعالجة الآلية للمعطيات دور الهدف، وتستهدف هذه الفئة من الجرائم نظام معالجة المعلومات نفسه، والمعلومات المخزنة فيه، أو المعطيات التي تتم معالجتها أو بعد مرحلة معالجتها، أو التي سيتم نقلها عبر الإنترنت من نظام معالجة إلى أخر، سواء كانت متصلة بهذا النظام أم ليست متصلة به، ويمكن تضمين أنواع مختلفة من الجرائم المتعلقة بالبريد الإلكتروني والاتصالات الإلكترونية في هذه الفئة. وما يتضح من خلالها أن الاتفاقية تجنبت تفصيل أنواع وأنماط السلوك الإجرامي أو الأشكال التي يمكن أن تتخذها الجريمة الواحدة، ويعتبر هذا النهج محمود لأنه في معظم الحالات يربط وصف السلوك بالوسائل الإلكترونية المستخدمة في ارتكاب الجريمة[2].

وما يلاحظ عليها كذلك أنه لم يحدد الإطار العام للنصوص الموضوعية في هذه الاتفاقية نوعية المعطيات والبيانات، ما إذا كانت معطيات شخصية تتصل بالشخص في حد ذاته، أو إقتصادية، أو مالية، أو أمنية، وهذا راجعاً إلى الرغبة في تعميم حماية البيانات والمعطيات بجميع أنواعها، لأن المعطيات الشخصية تحظى بتشريعات خاصة متميزة تتمثل في" الاتفاقية الأوروبية لحماية البيانات الشخصية" والأدلة الإرشادية الأوربية[3] ...الخ هذا ما سنفصل فيه لاحقا.

[1] أنظر المادة 6 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[2] مروة زين العابدين صالح، المرجع السابق، ص 439- 440.

[3] مروة زين العابدين صالح، المرجع نفسه، ص 440- 441.

ب_ الطائفة الثانية:

أما الطائفة الثانية وتتمثل في الجرائم المتصلة بالحاسب أو الكمبيوتر: ونصت عليها المادتان 7، 8 من هذه الإتفاقية على التوالي، فأولهما (المادة7) نصت على التزوير المعلوماتي والذي يُطلق عليه كذلك التزوير المتصل بالحاسب الآلي، أما الثانية (المادة 8) نصت على الغش المعلوماتي والذي يُطلق عليه كذلك الغش المتصل بالحاسب الآلي. وهذا النوع من الجرائم يكون فيه نظام المعالجة للحاسوب له دور الوسيلة، أي الأداة التي تستخدم لارتكاب جريمة تقليدية كالاحتيال والتزوير مثلا[1]. وقد ورد في التقرير التفسيري للاتفاقية حول هذه الجرائم أنه إذا كانت التشريعات القائمة في الدول تجرم هذه الأفعال الإجرامية التقليدية في نصوصها القانونية، وأن هذا التشريع واسع النطاق ويتضمن الحالات الجديدة التي تستخدم فيها شبكات الإنترنت، ففي هذه الحالة يكفي تطبيق القوانين السارية دون الحاجة إلى تعديل المواد التي تنص على هذه الجرائم التقليدية، واستحداث نصوص جزائية جديدة، ولكن إذا كانت هذه النصوص ضيقة وتنص فقط على هذه الجرائم في شكلها التقليدي، ولا يمكن أن تنطبق على هذه الأشكال الاجرامية المستحدثة، فعندئذ في هذه الحالة من الضروري تعديل هذه النصوص أو استحداث نصوص جديدة[2].

_ التزوير المعلوماتي: ويتمثل السلوك الاجرامي في هذه الجريمة في إنشاء أو تعديل البيانات المخزنة (دون الحصول على ترخيص، بحيث تكتسب قيمة إثباتية مختلفة في سياق المعاملات الوطنية التي تعتمد على دقة المعلومات الواردة في البيانات[3]. وهذه الجريمة عمدية.

_ الإحتيال المعلوماتي (الغش المعلوماتي): نصت عليه المادة 8 من نفس الإتفاقية، حيث تجرم هذه المادة أي شكل من أشكال التلاعب غير المشروع أثناء معالجة البيانات لغرض

[1] مروة زين العابدين صالح، المرجع السابق، ص 440.

[2] أنظر المادة 5 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[3] أنظر المادة 7 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

النقل غير المشروع للملكية. ويتمثل السلوك الإجرامي في هذه الجريمة في التلاعب بالبيانات المدخلة في نظام المعالجة، فيتم ادخال مجموعة بيانات غير صحيحة، أو من خلال التلاعب بالبرمجيات أثناء عملية المعالجة[1] .

وهذه الجريمة تعتبر جريمة عمدية، يتمثل القصد الجنائي العام فيها في التلاعب أو التدخل عبر الكمبيوتر، مما يؤدي إلى فقدان ملكية حساب شخص آخر، وتتطلب هذه الجريمة كذلك توافر نية إحتيالية أو نية الغش للمجرم المعلوماتي أو لغيره[2].

ج ـ الطائفة الثالثة: تتمثل في الجرائم المتصلة بالمحتوى، حيث نصت المادة 9 من الاتفاقية على هذه الجرائم والمتمثلة في الجرائم المتصلة بالمواد الإباحية للأطفال، فيمثل نظام المعالجة الآلية للكمبيوتر والإنترنت في هذا النوع من الجرائم بيئة رقمية إجرامية، وقد اقتصرت هذه الطائفة من الجرائم في هذه الاتفاقية على المواد غير الأخلاقية المتصلة بالأطفال أو المتعلقة بهم، ولم تنص على باقي أنواع جرائم المحتوى مثل المقامرة والمخدرات والجرائم ذات الصلة المرتبطة بها ومختلف الجرائم الأخرى[3].

ـ الجرائم المتصلة بالمواد الإباحية للأطفال: ويتمثل السلوك الاجرامي في كل فعل يتمثل في إنتاج وحيازة وتوزيع المواد الإباحية للأطفال أو إنتاج المواد المتعلقة بها بهدف توزيعها عن طريق نظام المعالجة الآلية للمعطيات.

أو عرضها أو توزيعها أو حيازتها بواسطة هذا النظام أو على دعامة تخزين، أو شرائها[4]، هذه الجريمة كذلك جريمة عمدية وتطلب نية عرض المواد الإباحية.

[1] أنظر المادة 8 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[2] أنظر المادة 8 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

[3] مروة زين العابدين صالح، المرجع السابق، ص 440.

[4] أنظر المادة 9 من التقرير التفسيري لإتفاقية الجريمة الإلكترونية.

د- الطائفة الرابعة: وتتمثل في الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة ونصت عليها المادة 10 من الاتفاقية.

_ الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة:

ويتمثل السلوك الإجرامي فيها في إستنساخ المصنفات المحمية بكل أنواعها ونشرها على الأنترنت دون الحصول على الموافقة من صاحبها الذي يتمتع بحق التأليف والنشر، وهذه تُرتكب عمدًا، ويعتبر نص المادة 10 نصا مكملا لقواعد الحماية الجنائية في مجال الملكية الفكرية والحقوق المجاورة التي تم وضعها وإقرارها على المستويين الوطني والدولي[1].

وتطرقت هذه الاتفاقية في بابها الثاني إلى الجوانب الإجرائية لهذه الجرائم.

وما يجدر بنا الإشارة إليه أن اتفاقية بودابست هي في الوقت الحاضر المرجع الدولي المعترف به لمكافحة جرائم الإنترنت والجرائم الأخرى ذات الصلة بالكمبيوتر. فبالإضافة إلى ذلك فهي تعتبر بمثابة آلية عالمية حيث ثلثا الدول تستخدم بالفعل اتفاقية بودابست علاوة على ذلك، فهي تعتبر آلية عالمية، يستخدمها ثلثي البلدان بالفعل في مكافحة هذه الجرائم[2].

بتاريخ 28 يناير سنة 2003 بستراسبورغ إستكملت الاتفاقية بالبرتوكول الإضافي الأول والذي أطلق عليه تسمية "البروتوكول الإضافي لإتفاقية الجريمة الالكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر" والهدف من هذا البرتوكول هو تكملة أحكام الشق الموضوعي الذي ورد في إتفاقية بودابست، فأحكام هذا البرتوكول تجرم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة المعالجة الآلية للمعطيات باعتبارها تعتبر وسيلة تُسهل حرية التعبير والتواصل في جل أنحاء العالم، لذلك تم إقرار هذا البروتوكول بغرض الموازنة بين حق حرية التعبير ومكافحة الأفعال التي طابعها عنصري قائم على كراهية

[1] مروة زين العابدين صالح، المرجع السابق، ص 440.

[2] Jan Kleijssen and Pierluigi Perri , Chapter 7 Cybercrime, Evidence and Territoriality: Issues and Options, Law 2016, Netherlands Yearbook of International Law 47, 2017, P168.

الأجانب[1]. ولأحكام هذا البرتوكول طابع إلزامي ويتوجب على الدول الأطراف من أجل الامتثال لهذه الالتزامات، ألا تكتفي بتشريع تشريعات وقوانين مناسبة، وإنما تضمن تنفيذها بشكل فعال[2].

ثم استكملت بالبروتوكول الإضافي الثاني والذي جاء كذلك ليكمل هذه الإتفاقية وموسوم بالبروتوكول الإضافي الثاني للإتفاقية المتعلقة بالجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية لسنة 2022.

فهذا البروتوكول يكمل كلا من إتفاقية بودابست، وبروتوكولها الأول[3]، تم اعتماده من طرف لجنة وزراء مجلس أوروبا، حيث بعد مرور 20 سنة على "إتفاقية بودابست"، وبغرض تكثيف التعاون وكشف الأدلة الرقمية، ويلاحظ أن هذا البرتوكول وسع من نطاق القانون ليشمل حتى الفضاء السيبراني، بهدف حماية مستخدمي الانترنت وضحايا الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وبغرض تسهيل جمع الأدلة الإلكترونية، ولتوفير أساسًا قانونيًا، للكشف عن معلومات تسجيل اسم النطاق[4]، ولتجسيد صورة من صور التعاون المباشر مع مزودي الانترنت لتحصل على المعلومات المتعلقة بالمشتركين، وأرقام وحروف

[1] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, European Treaty Series - No. 189, Conseil of L'Europe, Strasbourg, 28 .I. 2003. available at: https://rm.coe.int/168008160f

[2] أنظر إلى التعليق على المادة 1، التقرير التفسيري للبروتوكول الإضافي لإتفاقية الجريمة الالكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، سلسلة المعاهدات الأوربية رقم 169، مجلس أوربا، الصادر بستراسبورغ بتاريخ 28 يناير/ كانون الثاني 2003، الوثيقة منشورة على الرابط التالي: https://rm.coe.int/explanatory-report-additional-protocol-on-xenophobia-and-racism-in-ara/1680739176

[3] أنظر المادة 1 من البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية الصادر عن مجلس أوربا سنة 2021.

[4] مثلا DZ هذا الرمز يرمز إلى أن عنوان المواقع على شبكة الأنترنت على أنها في الجزائر. أنظر هاني الحبال، قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، د.د.ن، بيروت، 2019، ص60.

ورموز المرور، والتعاون الفوري عند حالة الطوارئ، وآليات المساعدة المتبادلة، إضافة إلى ضمانات حماية البيانات الشخصية[1].

ثانيا: دور الاتفاقية الأوربية المتعلقة بالجريمة المعلوماتية وأهميتها في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تعتبر في وقتنا الحالي الاتفاق الوحيد المكرس فعلا بشكل ملزم وذو فاعلية على الصعيد الدولي، كونها ثمرة جهد متواصل طيلة أربعة سنوات للجنة من الخبراء تدعى " لجنة الخبراء بشأن الجريمة في الفضاء الإفتراضي" هؤلاء الخبراء تابعين لمجلس أوروبا، وبمساعدة خبراء من غير الدول الأعضاء في المجلس الأوربي كاليابان وكندا والولايات المتحدة الإمريكية، وخبراء من جنوب إفريقيا[2].

_ أكدت على ما تم إنجازه من جهود في مجال الجرائم المعلوماتية من طرف الأمم المتحدة ومنظمة التعاون الإقتصادي والتنمية والاتحاد الأوروبي كونها تعتبر حصيلة ونتيجة لمختلف الجهود الدولية والإقليمية.

_ السعي نحو تحقيق وحدة التدابير التشريعية الموضوعية بين الدول الأوروبية والدول المنظمة للاتفاقية من الدول الأوروبية، وكذلك الإجرائية والتي تكون متناسبة وطبيعة الجرائم المعلوماتية، وأكدت كذلك على أهمية تظافر الجهود الدولية والاقليمية في مجال مكافحة هذا النوع من الإجرام[3]، لأنه بدون التعاون الدولي لن يكون هناك أثر لأي مجهود تقوم به أي

[1] Official Council of Europe website,"Second Additional Protocol to the Budapest Convention adopted by the Committee of Ministers of the Council of Europe", Strasbourg, 17 November 2021, available at: https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe
Accessed September 20, 2022 At 09 :28.

[2] مناصرة يوسف، المرجع السابق، ص 297.

[3] مروة زين العابدين صالح، المرجع السابق، ص 442- 443.

دولة من الدول بمفردها، لأن تلك الجرائم تكون في الأغلب الأعم من الحالات جرائم عابرة للحدود[1].

وإيجاد مرجعية ودليل إرشادي للتدابير التشريعية الوطنية في مجال مكافحة الجريمة المعلوماتية، ضف إلى ذلك أكدت على ضرورة فعالية خطط العمل لمكافحة الأنشطة التي تستهدف سرية وسلامة المعلومات والأنظمة وشبكات الكمبيوتر، بما فيها تحديد كل من الإطار الموضوعي والإجرائي لهذه الأنشطة، على المستويين الوطني والدولي.

_ وأكدت على ضرورة تحقيق التوازن بين حماية حقوق الإنسان الأساسية والمعترف بها بموجب مواثيق دولية (كاتفاقية مجلس أوروبا لحماية حقوق الإنسان وحريته الأساسية لعام 1950 والعهد الدولي للحقوق المدنية والسياسية لعام 1966 والاتفاقيات العالمية الأخرى في ميدان حقوق الإنسان)، والحقوق المرتبطة بالرأي وحرية الوصول للمعلومات وحرية البحث والتلقي والنقل للمعلومات والأفكار، وبين الحق في الخصوصية وحيازة المعلومات والاستفادة من عناصر الملكية الفكرية لها، وهذا المنطلق يمثل النظرة الفلسفية الحكمية للجرائم المعلوماتية ووجوب الحماية منها دون الوصول إلى مدى تتأثر فيه حقوق الأفراد بالوصول إلى المعلومات أو تتأثر من أنشطة الاحتكار والاستغلال غير المشروع للمعرفة[2].

_ وحدت مختلف الإجراءات القانونية المتعلقة بالبحث والتحري عن مرتكبي الجرائم المعلوماتية.

_ توفير نظام سريع وفعال للتعاون الدولي.

_ عززت أُطر التعاون على المستوى الاقليمي والدولي والاقليمي من خلال انضمام الدول إليها وتسليم المجرمين ومنعهم من الفرار.

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 22.

[2] مروة زين العابدين صالح، المرجع نفسه، ص 442- 443.

_جعلت الدول تواءم بين تشريعاتها الداخلية ونصوص الاتفاقية[1].

ويتضح مما سبق أن هذه الاتفاقية شُرعت بغرض التصدي المشترك للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والتنسيق، لأن الجهود الفردية للدول في مكافحتها غير كافية، وذلك لعبورها الحدود الوطنية، ما يعكس توجه الدول حتى غير الأعضاء في مجلس أوربا وانضمامهم الى هذه الاتفاقية، فخطورة هذه الجريمة غيرت التصور الاتفاقي على المستوى العالمي، حيث يكمن الهدف الأساسي لاتفاقية بودابست في مواءمة التشريعات الداخلية مع ما ورد فيها، بهدف ضمان حماية من تهديدات هذه الجرائم.

فاتفاقية بودابست جسدت سياسة جنائية مشتركة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، تتبلور من خلال تبني مضمونها وموائمة التشريعات الوطنية للدول معها، من خلال تجريم الأفعال التي جرمتها الاتفاقية، وتحديد عقوبات لها حسب تشريع كل دولة، وتعزيز التعاون الدولي.

وما يجدر بنا الاشارة إليه في هذا الصدد أن الجزائر لم تصادق على إتفاقية بودابست، لكن المشرع الجزائري تبنى مضمون هذه الاتفاقية ضمن قانون العقوبات، وجرم الأفعال التي نصت عليها هذه الإتفاقية، وبالتالي المشرع الجزائري استفاد من مضمونها دون التقييد بها ودون ترتيب مسؤولية دولية على مخالفتها .

فالجزائر لم تصادق على هذه الاتفاقية لاعتبارات سياسية، وذلك لعدم توافق مضمون هذه الاتفاقية مع السياسة العامة للدولة، والالتزامات الاقليمية وخاصة أن الجزائر لا تنمتي لدول الاتحاد الأوربي.

[1] Convention sur la cybercriminalité, Série des traités européens - n° 185, Conseil de l' Europe, Budapest, 23.XI.2001.

الفرع الثاني: تشريعات مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى العربي

تكاثفت الجهود التشريعية كذلك على المستوى الإقليمي العربي من خلال سن العديد من التشريعات العربية الإقليمية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أهمها: قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها (أولا)، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات (ثانيا).

أولا: قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها

انعقد بتونس بتاريخ 2003/3/10 الاجتماع (11) للجنة الجرائم المستجدة، الذي تمحور حول موضوع الجرائم المستجدة وكيفيات مواجهتها، وكانت أهم التوصيات الصادرة عنه وضع مشروع إتفاقية عربية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وبناءًا على ما سبق أعدت اللجنة المشتركة لمجلس وزراء الداخلية والعدل العرب، التي اجتمعت في دولة تونس في الفترة ما بين21 و22 مايو 2003، وتمت الموافقة على مشروع قانون عربي إسترشادي لمكافحة جرائم المعلوماتية، خلال الدورة التاسعة عشرة (19) لمجلس وزراء العدل لجامعة الدول العربية المنعقد في دولة الجزائر من 8 إلى 9 أكتوبر 2003[1].

تم اعتماده من طرف مجلس وزراء العرب في الدورة (19) التاسعة عشر بموجب القرار رقم (495/ د19)[2] بتاريخ 8 أكتوبر 2003، ومن طرف مجلس وزراء الداخلية العرب في دورته (21) الحادية والعشرين، التي انعقدت في تونس بتاريخ 4-2004/1/5م[3]، وبموجب القرار رقم (417- د21/ 2004)[4]، بعد تعديل تسميته إلى "قانون الإمارات العربي الاسترشادي

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 29- 30.

[2] فاروق خلف، المرجع السابق، ص 15.

[3] رامي متولي القاضي، عمر سالم، المرجع نفسه، ص 30.

[4] فاروق خلف، المرجع نفسه، ص 15.

لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها[1]" وتقرر تعميمه على جميع الدول العربية للاستفادة منه[2]. ويحتوي هذا القانون على 27 مادة تتضمن التجريم والعقاب على ارتكاب الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات[3]، وما تجدر بنا الإشارة إليه أن أجهزة الأمانة العامة لمجلس وزراء الداخلية العرب تسعى جاهدة لتبني استراتيجية عربية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لاتزال قيد الإعداد حتى كتابة هذه السطور[4].

ثانيا: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

توجت جهود جامعة الدول العربية في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بالتوقيع في نهاية عام 2010 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والتي هدفها الأساسي تعزيز التعاون بين الدول العربية في مجال مكافحة الجرائم المعلوماتية، وتتكون هذه الإتفاقية من 43 مادة، وتتضمن أحكامًا موضوعية وأخرى إجرائية[5].

وقُسمت هذه الاتفاقية إلى 4 فصول، الفصل الأول منها عُنون بأحكام عامة، تضمن 4 مواد من المادة الأولى إلى المادة الرابعة.

المادة الأولى منها نصت على الهدف من الاتفاقية والمتمثل في تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة هذا النوع من الجرائم، وذلك بهدف درء أخطار هذه الجرائم

[1] أطلقت عليه تسمية قانون الإمارات الاسترشادي العربي لمكافحة جرائم تقنية المعلومات وما في حكمها نسبة إلى دولة الامارات العربية التي اقرحته.

[2] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 30.

[3] فاروق خلف، المرجع السابق، ص 15.

[4] رامي متولي القاضي، عمر سالم، المرجع نفسه، ص 30.

[5] رامي متولي القاضي، عمر سالم، المرجع نفسه، ص 31.

والحفاظ على أمن الدول العربية ومصالحها وسلامة مجتمعها وأفرادها[1]، أما المادة الثانية منه تضمنت المصطلحات الواردة في هذه الاتفاقية والمقصود بها، وذلك لأجل إزالة الغموض وتوضيح معانيها، حتى لا يكون هناك لبس يشوب تطبيق هذه الاتفاقية بالنسبة للدول المصادقة عليها، وكذلك حتى لا يكون هناك لبس بالنسبة للدول التي تريد المصادقة عليها، والمصطلحات التي تم شرحها فيها هي: تقنية المعلومات، ومزود الخدمة، والبيانات، والبرنامج المعلوماتي، النظام المعلوماتي، الشبكة المعلوماتية، الموقع، الالتقاط ومعلومات المشترك[2]، وحسنا فعلت الدول المُنشِأة لهذه الإتفاقية بشرحها هذه المصطلحات لأنها مصطلحات تقنية تتطلب شرحها ووضع مفهوم موحد لها، لأنه قد يختلف مفهومها من دولة إلى أخرى.

أما بالنسبة للمادة الثالثة منها فنصت على مجالات تطبيق هذه الإتفاقية، حيث يتم تطبيقها على الجرائم المعلوماتية بغرض منعها والتحقيق فيها ومتابعة مرتكبيها في 4 حالات حددتها على سبيل الحصر وهي: إذا إرتُكبت جرائم تقنية المعلومات في أكثر من دولة، أو إذا إرتُكبت في دولة وتم التخطيط لها وتوجيهها أو الاشراف عليها في دولة أو دول أخرى، أو إذا تم إرتكابها في دولة من طرف مجموعة إجرامية منظمة ترتكب جرائمها وسلوكاتها المُجرمة في أكثر من دولة، وكذلك في الحالة التي ترتكب فيها في دولة وتتعدى أثارها الشديدة والخطيرة حدود الدولة الواحدة[3]، أي لابد أن تكون الجريمة عابرة للحدود ولا تقف في دولة واحدة، وإنما تمس أكثر من دولة عربية.

[1] أنظر المادة 01 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، القاهرة، 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة عام 1435 الموافق ل 8 سبتمبر 2014، ج. ر.ج.ج العدد57، المؤرخة في 28 سبتمبر 2014.

[2] للإطلاع على شرح هذه المصطلحات أنظر المادة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] أنظر المادة 03 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

أما المادة الرابعة من الاتفاقية فنصت على مبدأ دستوري مهم يكون في دساتير الدول وفي قوانينها الأساسية وهو مبدأ صون السيادة، وعدم التدخل في الشؤون الداخلية لتلك الدول[1].

وبخصوص الفصل الثاني فتمت عنونته بالتجريم، يتكون من 17 مادة، من المادة 5 إلى المادة 21 من الاتفاقية السالفة الذكر.

حيث نصت المادة الخامسة منها على وجوب تجريم الأفعال الواردة في هذا الفصل من قبل الدول الأطراف في هذه الإتفاقية في تشريعاتها وقوانينها الداخلية[2].

أما المواد من المادة 6 إلى المادة الثامنة عشر على التوالي حددت الأفعال المجرمة في الإتفاقية والمتمثلة في جريمة الدخول غير المشروع (المادة 6)، جريمة الاعتراض غير المشروع (المادة7)، جريمة الإعتداء على سلامة البيانات(المادة 8)، جريمة إساءة إستخدام وسائل تقنية المعلومات (المادة 9)، جريمة التزوير (المادة 10)، جريمة الاحتيال (المادة 11)، جريمة الإباحية (المادة 12)، الجرائم الأخرى المرتبطة بالإباحية (المادة 13)، جريمة الإعتداء على حرمة الحياة الخاصة (المادة 14)، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات (المادة 15)، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات (المادة 16)، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة (المادة 17)، الاستخدام غير المشروع لأدوات الدفع الالكترونية (المادة 18).

فهذا الفصل تم تحديد فيه مجموع الجرائم والأفعال التي تشكل جرائم تقنية المعلومات، ضف إلى ذلك تجريم الشروع والاشتراك في إرتكاب جريمة من الجرائم التي سبق ذكرها الواردة في هذا الفصل (المادة 19)، وتم إقرار المسؤولية الجزائية للشخص المعنوي عن الجرائم التي يرتكبها ممثله باسمه ولصالحه، مع معاقبة الشخص الطبيعي (المادة 20)، وتم

[1] أنظر المادة 04 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] أنظر المادة 05 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

النص فيه كذلك على تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات (المادة 21).

أما الفصل الثالث منها فجاء موسوم بالأحكام الإجرائية، يتكون من 8 مواد من المادة 22 إلى المادة 29 من الاتفاقية، أما الفصل الرابع منها جاء موسوم بالتعاون القانوني والقضائي فإنه يتكون من 13 مادة من المادة 30 إلى المادة 43. أما الفصل الخامس والأخير فوردت فيه أحكام ختامية.

وما يجب الإشارة إليه أنه صادقت الجزائر على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بتاريخ 8 سبتمبر 2014[1].

ولهذه الإتفاقية "الإتفاقية العربية لمكافحة جرائم تقنية المعلومات" دور وأهمية كبيرة كونها تميزت عن إتفاقية بودابست بنصها على جرائم جديدة كالإرهاب السيبراني، والاستخدام غير المشروع لأدوات الدفع الالكتروني كتزوير أو تقليد أدوات الدفع الالكترونية، أو الاستلاء على معطيات أدوات الدفع، أو استخدام الانترنت بدون حق للوصول إلى أرقام وبيانات ومعطيات أدوات الدفع...، وكذلك أضافت جريمتي المقامرة والاستغلال الجنسي وجريمة الاعتداء على حرمة الحياة الخاصة.

وما ميزها كذلك عن اتفاقية بودابست هو أنها كرست نوع مستحدث من السيادة يتمثل في السيادة السيبرانية للدول التي انضمت إليها فكل دولة تتمتع بسيادتها على مستوى فضائها السيبراني، وعدم قابلية التدخل فيه إلا من خلال الآليات القانونية المتعارف عليها، دون السماح للدول الأطراف فيها من التدخل المباشر في الفضاء الرقمي لدولة أخرى عن طريق إجراء تحقيقات فيه عن بعد، على النحو المنصوص عليه في الإتفاقية السالفة

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، القاهرة، 21 ديسمبر 2010، المصادق عليها من طرف الجزائر بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة عام 1435 الموافق ل 8 سبتمبر 2014، ج. ر.ج.ج العدد57، المؤرخة في 28 سبتمبر 2014.

الذكر[1]، ويتمثل دورها أيضا في أنها أكدت على تعزيز التعاون بين الدول الأطراف لمكافحة هذا النوع من الإجرام الذي يهدد أمنها ومصالحها.

وأكدت على تبني سياسة جنائية مشتركة بين الدول العربية المنضمة للاتفاقية لمكافحة جرائم تقنية المعلومات، وأكدت على احترام حقوق الانسان ومختلف الحقوق المكفولة بموجب مواثيق دولية وعربية[2].

المطلب الثاني: التشريعات الدولية الخاصة بحماية المعطيات الشخصية

أصبحت التكنولوجيا والرقمنة اليوم تغزو العالم، حيث صارت غالبية المعاملات تشترط الحصول على المعطيات الشخصية، وهذا رافقته العديد من المخاطر التي تؤثر سلبا على الحياة الشخصية للأفراد، ما أدى إلى ظهور مفهوم جديد في الساحة القانونية، وهو حماية المعطيات الشخصية فظهور هذه الفكرة مرتبطا ارتباط مباشرا بتطور تكنولوجيا المعلومات[3]، وثار جدل فقهي حول ارتباط الخصوصية بالمعطيات الشخصية، واتفقت المدارس الفقهية الحالية حول أن حماية المعطيات الشخصية نشأت من حماية الحق في الخصوصية[4]. حيث في البداية تجسدت الحماية الجنائية للمعطيات الشخصية ضمن نطاق الحماية الجنائية للحق في الحياة الخاصة على المستوى الدولي فتمت حماية هذا الحق بموجب المواثيق والصكوك الدولية، حيث توجد صكوك دولية وضعت البوادر الأولى لحماية المعطيات الشخصية، لكن لا توجد هناك إتفاقية دولية متخصصة في هذا الشأن، ومن هذه الصكوك والمواثيق الإعلان

[1] مناصرة يوسف، المرجع السابق، ص 316- 317.

[2] أنظر ديباجة الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] Wassila Kannoufi , Protection des données à caractère personnel : Un cadre juridique en évolution Protection of Personal Data: An Evolving Legal Framework, Journal of letters and Social Sciences, Vol 19, N° 02 , 2022, P316.

[4] Olumide Babalola, Nigeria's data protection legal and institutional model: an overview, International Data Privacy Law, Vol. 12, No. 1 ,2022 ,P45.

العالمي لحقوق الإنسان[1]، بموجب م 12 منه[2]، وكذلك العهد الدولي للحقوق المدنية والسياسية[3] بموجب م 17[4]منه، وكذلك إتفاقية حقوق الطفل[5].

(La convention internationale des droits de l'enfant) كرست حماية لمعطيات الطفل الشخصية بموجب نص المادة 16[6]، وما يجدر بنا الإشارة إليه في هذا الصدد أن هذه الاتفاقية صادقت عليها الجزائر[7].

استنادا لذلك، سيتم التطرق للتشريعات المتعلقة بحماية المعطيات الشخصية على المستوى الأوروبي (كفرع الأول)، والتشريعات المتعلقة بحماية المعطيات الشخصية على المستوى الافريقي (كفرع الثاني).

---

[1] تجلى عن إجتماعات لجنة حقوق الانسان التابعة للأمم المتحدة إصدار اتفاق للحقوق والحريات الأساسية والمعروف بالإعلان العالمي لحقوق الإنسان، وقد وافقت الجمعية العامة للأمم المتحدة عن هذا الإعلان في قرارها رقم 712 الصادر خلال دورتها العادية الثالثة في 1948/12/10، واهتم هذا الاعلان بالحياة الخاصة، أنظر علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، 2020، ص 57- 58.

[2] تنص المادة 12 من الاعلان العالمي لحقوق الإنسان الذي اعتمد بموجب قرار الجمعية العامة للأمم المتحدة رقم 217 ألف، الدورة 3، المؤرخ في 10 ديسمبر 1948 على أنه: " لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو سكنه أو مراسلاته أو الحملات على شرفه أو سمعته، ولكل شخص الحق في الحماية القانونية من قبل هذا التدخل أو تلك الحملات".

[3] العهد الدولي للحقوق المدنية والسياسية، الذي اعتمد بموجب قرار الجمعية العامة للأمم المتحدة رقم 2200 ألف، الدورة21، المؤرخ في 16 ديسمبر 1966.

[4] المادة 17 من العهد الدولي للحقوق المدنية والسياسية " لا يجوز التدخل بشكل تعسفي أو غير قانوني بخصوصيات أحد أو بعائلته أو مراسلاته كما لا يجوز التدخل بشكل غير قانوني لشرفه وسمعته"

[5] إعتمدت وعُرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 25/44 المؤرخ في 20 تشرين الثاني/ نوفمبر ، 1989 وتاريخ بدء نفاذها هو 2 أيلول/ سبتمبر 1990.

[6] المادة 16 من إتفاقية حقوق الطفل " لا يجوز أن يجرى أي تعرض تعسفي أو غير قانوني للطفل في حياته الخاصة أو أسرته أو منزله أو مراسلاته، ولا أي مساس غير قانوني بشرفه أو سمعته ".

[7] تمت المصادقة عليها بموجب المرسوم الرئاسي رقم 92- 461 بتاريخ 1992/12/19 الجريدة الرسمية عدد 91 بتاريخ 23 ديسمبر 1992.

الفرع الأول: التشريعات المتعلقة بحماية المعطيات الشخصية على المستوى الأوروبي

تعتبر الاتفاقية الأوروبية لحقوق الانسان والحريات الأساسية هي أول إتفاقية مهدت إلى حماية المعطيات الشخصية على المستوى الأوربي، حيث نصت المادة 8[1]، منها على الحق في إحترام الحياة الخاصة والعائلية، ثم بعدها ظهرت العديد من التشريعات الدولية في أوربا على مستوى كل من المجلس الاوروبي، وعلى مستوى الإتحاد الأوروبي.

فمن خلال هذا الفرع سنتطرق إلى التشريعات الدولية المتعلقة بحماية المعطيات الشخصية على مستوى المجلس الاوروبي (أولا)، التشريعات الدولية المتعلقة بحماية المعطيات الشخصية على مستوى الإتحاد الأوروبي (ثانيا).

أولا: التشريعات المتعلقة بحماية المعطيات الشخصية على مستوى المجلس الاوروبي

1 _ الاتفاقية المتعلقة بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية (الاتفاقية رقم 108 لمجلس أوروبا):

يطلق عليها كذلك تسمية إتفاقية ستراسبورغ، وتُسمى كذلك الإتفاقية رقم 108لمجلس أوربا بالنظر إلى رقمها، تم التوقيع عليها بتاريخ 28 جانفي1981 بستراسبورغ، بغرض ضمان إضفاء حماية على الحياة الخاصة للأفراد في مواجهة إستخدام البيانات الشخصية آليًا[2]، تحت مظلة لجنة وزراء من المجلس الأوروبي تختص بموضوع الخصوصية[3]، وأصبحت هذه

---

[1] المادة 8 من الإتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، الصادرة عن المجلس الأوربي، الموقعة في روما بتاريخ 04 نوفمبر 1950. " – لكل شخص الحق في إحترام حياته الخاصة والعائلية ومسكنه ومراسلاته.

_ لا يجوز أن تتدخل السلطة العامة في ممارسة هذا الحق إلا إذا نص القانون على هذا التدخل، وكان ضروريا، في مجتمع ديمقراطي، لحفظ سلامة الوطن، أو الأمن العام، أو الرخاء الإقتصادي للبلد، أو لحفظ النظام، أو لمنع الجرائم، أو لحماية الصحة والأخلاق، أو لحماية حقوق الآخرين وحرياتهم".

[2] بنور سعاد، حماية الحياة الخاصة للعامل، أطروحة للحصول على شهادة دكتوراه علوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة وهران 2، 2016/ 2017، ص 65.

[3] بنور سعاد، المرجع نفسه، ص 65.

الإتفاقية نافذة بتاريخ 1985 /10/01، وقد وقعت على هذه الإتفاقية 31 دولة صادق منها 21 دولة عليها، وبقيت عشرة دول غير مصادقة وفقا لواقع الإتفاقية بتاريخ 2000/01/31[1]، ومن الدول الموقعت عليها فرنسا، بلجيكا، النمسا، الدنمارك، إيطاليا...[2].

فهذه الاتفاقية أوجدت حق أساسي جديد، يتمثل في حق حماية البيانات الشخصية للفرد خلال مراحل معالجتها أينما كانت موجودة[3].

ورد في هذه الإتفاقية ديباجة و27 مادة.

الفصل الأول من هذه الإتفاقية عُنون بأحكام عامة، نصت المادة الأولى منه على هدف هذه الإتفاقية والمتمثل في حماية الحق في الخصوصية فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية[4]، أما المادة الثانية فعرفت مجموعة من المصطلحات وهي: البيانات الشخصية، ملف البيانات الآلي، المعالجة الآلية، مراقب الملف[5].

---

[1] مروة زين العابدين صالح، المرجع السابق، ص 301.

[2] بنور سعاد، المرجع السابق، ص 65.

[3] Cesare Parodi, Valentina Sellaroli, op cit, p718 .

[4] Art 01 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne, Série des traités européens - n° 108 , Conseil de l' Europe, Strasbourg, 28.I.1981.

« Art 1er – Objet et but

Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données».

[5] Art 02 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

« Art 2 – Définitions

Aux fins de la présente Convention:

a «données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);

b «fichier automatisé» signifie: tout ensemble d'informations faisant l'objet d'un traitement automatisé;

c «traitement automatisé» s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;

d «maître du fichier» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées. »

أما المادة الثالثة منها فحددت نطاق هذه الإتفاقية، والإلتزامات الدول المنظمت لها بتطبيقها على المعطيات الشخصية المعالجة آليا في القطاعين العام والخاص، ونصت كذلك على أن هذه الاتفاقية لا يمكن تطبيقها على فئات معينة من البيانات الشخصية[1]، أما الفصل الثاني منها فنص على المبادئ الأساسية لحماية البيانات، حيث في المادة الرابعة تم النص على إلتزامات الدول الأطراف، فنصت على أهم إلتزام يقع على عاتق الدول المصادقة عليها وهو ضرورة سن تشريعات داخلية تتضمن الإجراءات الضرورية التي تحقق الغرض من هذه الاتفاقية والمتمثل في حماية المعطيات الشخصية وفقا للمبادئ المنصوص عليها في هذا الفصل، ويتم تطبيقها في أجل أقصاه تاريخ نفاذ هذه الاتفاقية[2]، أما المادة الخامسة منه نصت على المبادئ الأساسية الواجب توافرها في البيانات التي يتم معالجتها، والمتمثلة في المشروعية وتحديد الغرض، وتكون كافية وغير مفرطة، ودقيقة ومحدثة عند الاقتضاء، وتكون مخزنة لمدة محددة تتوافق مع الغرض الذي يتم معالجتها لأجله[3].

أما المادة السادسة منه نصت على البيانات التي لا يمكن معالجتها إلا إذا وفر القانون الوطني لتلك الدولة ضمانات كافية نظرا لطبيعة هذه المعطيات الخاصة وحساسيتها كالمعتقدات التي تبين الأصل العرقي والمعتقدات الدينية والآراء السياسية...الخ[4]، أما المادة السابعة منه نصت على أمن البيانات والذي يكون من خلال إتخاذ مختلف التدابير الأمنية المناسبة لغرض حماية البيانات الشخصية من التدمير أو الفقد العرضي أو الوصول غير المصرح به أو التغيير أو النشر[5]، أما المادة الثامنة منه فنصت على ضمانات أخرى يتمتع

[1] Art 04 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[2] Art 04 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[3] Art 05 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[4] Art 06 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[5] Art 07 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

بها صاحب البيانات[1]، أما المادة التاسعة منها فنصت على الإستثناءات إلا أنها إستثنت المادة 5 التي جاءت بالمبادئ والمادة 6 التي نصت على فئة المعطيات الخاصة، أما المادة الثامنة نصت على الضمانات التي يتمتع بها صاحب البيانات. ونصت عن الحالات التي يمكن فيها الخروج عن القواعد التي نصت عليها هذه المواد (5، 6، 8)[2]، أما المادة 10 منها فنصت على وجوب سن عقوبات في التشريعات الوطنية للدول الأطراف إذا ما لم يتم التقيد بالمبادئ الواردة في هذا الفصل[3]، أما المادة 11 منها نصت على إمكانية تمديد الحماية، حيث يمكن للدول الأطراف في هذه الاتفاقية النص على حماية أكثر من الحماية الواردة في الاتفاقية، لأن هذه الأحكام لا يمكن تفسيرها على أنها تقيد الحماية حسبما ورد في الاتفاقية فقط[4]، أما الفصل الثالث من هذه الاتفاقية فجاء تحت عنوان تدفقات البيانات عبر الحدود.

فالمادة 12 منه نصت على تدفقات البيانات عبر الحدود والقانون الوطني (المحلي)، حيث تنطبق أحكام هذه الاتفاقية على البيانات التي تخضع للمعالجة الآلية أو التي تم تجميعها بغرض معالجتها آليا، المنقولة عبر الحدود الوطنية بأي طريقة كانت، وبينت أحكام نقل هذه البيانات إلى دول أخرى سواء كانت طرف أو غير طرف في هذه الاتفاقية[5].

أما الفصل الرابع موسوم بالمساعدة المتبادلة، نصت المادة 13 منه على التعاون بين الأطراف وبينت أحكامه[6]، والمادة 14 منه نصت على المساعدة لأصحاب البيانات المقيمين بالخارج، وبينت أحكامها وبينت البيانات الإلزامية الواجب ورودها في طلب المساعدة

[1] Art 08 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.
[2] Art 09 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.
[3] Art 10 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.
[4] Art 11 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.
[5] Art 12 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.
[6] Art 13 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

والمتمثلة في الإسم واللقب والعنوان وأي بيان يحدد هوية مقدم الطلب، وملف البيانات الشخصية المعالجة آليا الذي يتعلق به الطلب، والغرض من الطلب[1]، أما المادة 15 منه فنصت على الضمانات المتعلقة بالمساعدة المقدمة من قبل السلطات المختصة[2]، أما المادة 16 فنصت على الحالات التي يتم فيها رفض طلبات المساعدة، حيث أنه في الأصل لايجوز رفض الطلبات، وإستثناء يجوز رفضها وذلك في حالات حددتها هذه المادة على سبيل الحصر[3]. أما المادة 17 منها فنصت على تكاليف وإجراءات المساعدة[4].

وما يجدر بنا الإشارة إليه أنه يوجد كذلك برتوكول اضافي لهذه الاتفاقية.

وما تمت ملاحظته بخصوص هذه الإتفاقية أنها نظمت المعالجة الالكترونية للبيانات ذات الصبغة الشخصية من خلال نصوصها، وحددت أهم مبادئها بالرغم من أنها لم تنص على جميع المبادئ الواجب توافرها، نصت كذلك على المعطيات الحساسة التي لا تخضع لهذه الإتفاقية، إضافة إلى ذلك أضفت هذه الإتفاقية حماية البيانات على المستوى الدولي في حالة تدفقها عبر الحدود، وتعاون الدول الأطراف فيها وتبادل المساعدة بينهم.

وتبعا لما سبق فإنه هذه الإتفاقية تشكل أول نموذج قانوني في مجال حماية المعطيات الشخصية.

[1]Art 14 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[2] Art 15 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[3] Art 16 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

[4] Art 17 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne.

ثانيا: التشريعات المتعلقة بحماية المعطيات الشخصية على مستوى الإتحاد الأوروبي

1 _ توجيه حماية البيانات EC/95/46:

التوجيه رقم 46/ 95/ EC الصادر عن البرلمان الأوربي والمجلس بتاريخ 24 أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وبشأن حرية حركة تلك البيانات:

على الرغم من النجاح الذي حققه مجلس أوروبا في إرساء حماية للبيانات وتحديد العناصر الأساسية للإطار القانوني لهذه الحماية، إلا أنه لم يضمن الإتساق الكافي بين الدول الأعضاء في تنفيذ الإتفاقية رقم 108 – التي سبق التطرق إليها– وكذلك في بعض الاحيان تم فرض قيود على تدفق البيانات إلى الدول الأعضاء الأخرى، لذا تم إرساء هذا التوجيه بغرض تحقيق إتساق وموائمة في القوانين الوطنية بشأن حماية البيانات في القطاع الخاص والعام[1].

حيث تهدف مبادئ هذا التوجيه إلى حماية الحقوق والحريات الأساسية خلال معالجة البيانات الشخصية، فيسعى هذا التوجيه إلى تحقيق هدف مزدوج من خلال فرضه إلتزامين على الدول الأعضاء، يتمثل الأول في أنه يتطلب من جميع الدول الأعضاء حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، ولاسيما الحق في الخصوصية فيما يتعلق بمعالجة البيانات الشخصية وفقا لهذا التوجيه، والهدف الثاني يتطلب منهم عدم تقييد أو حظر التدفق الحر للبيانات الشخصية فيما بين الدول الأعضاء لأسباب مرتبطة بهذه الحماية، فكلا من

[1] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, p 09. See information available at: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf . accessed September 26 , 2022 At 08 :30.

الإلتزامين مرتبط بالأخر ووثيق الصلة به، بغرض تحقيق مستوى عال من الحماية لجميع الأعضاء الدول[1].

_ تمت تكملته بتوجيه 58/ 2002 EC " توجيه الخصوصية الإلكترونية":

حيث في 12 يوليو 2002 أصدر المشرع الأوروبي هذا التوجيه رقم (58/ 2002 EC) والخاص بمعالجة البيانات ذات الطابع الشخصي والحياة الخاصة في إطار الانترنت والعمل به[2].

2_ النظام العام الأوروبي لحماية المعطيات الشخصية " General Data Protection Regulation":

في يناير لسنة 2012 تم إقتراح لتعديل وإصلاح الهيكل القانوني لحماية الخصوصية في أوروبا، وذلك بغرض تجنب التناقضات المتواجدة في القوانين الوطنية، والرفع من مستوى الحماية لخصوصية الأفراد، وكذلك عصرنة القوانين بغرض التماشي مع تحديات الخصوصية المعاصرة، مثل تلك التي تطرحها الأنترنت ووسائل التواصل الإجتماعي والتطبيقات المتوافرة بالأجهزة المحمولة والحوسبة السحابية والبيانات الضخمة التي لم تكن موجودة عندما تمت صياغة توجيه حماية البيانات، وكذلك بغرض تقليل الأعباء الإدارية ذات الكلفة الباهضة التي تدفعها الشركات التي تتعامل مع هيئات حماية البيانات المتعددة، لذا إقترحت اللجنة إستبدال توجيه 1995 بلائحة عامة لحماية البيانات، والتي وافق عليها المجلس الأوربي والبرلمان بعد مناقشات وحوارات مكثفة حول دقة محتوى هذه اللائحة العامة لحماية البيانات، وتم التناقش كذلك عن توجيه منفصل يبين أحكام التعاون الدولي للشرطة والتعاون القضائي في المسائل الجنائية[3]، يطلق عليها تسمية لائحة GDPR هي إختصار

[1] Peter Hustinx, op.cit , p 09.

[2] عمار عباس الحسيني، جرائم الحاسوب والإنترنت الجرائم المعلوماتية دراسة مقارنة في تشريعات: أمريكا وفرنسا والسويد وإنكلترا والسعودية والسودان، ط 2، منشورات زين الحقوقية، بيروت، لبنان، 2019، ص 236.

[3] W.Scott Blackmer Getting Ready for the New EU General Data Protection Regulation, 5 May, 2016,

ل: General Data Protection Regulation وهو نظام في الإتحاد الأوربي يختص بحماية البيانات والخصوصية لجميع الأفراد داخل الإتحاد الأوربي، ويعالج كذلك مسألة تدفق المعطيات الشخصية خارج الدول التابعة للإتحاد الأوربي، فالهدف الأساسي من هذا النظام هو تمكين المواطنين الأوربيين والمقيمين في أوربا من السيطرة والتحكم في بياناتهم الشخصية، ويهدف كذلك هذا النظام إلى تبسيط مجال التنظيمات والقوانين للمشاريع التجارية ذات الطابع الدولي وذلك من خلال توحيد التنظيمات والتشريعات الأوربية، حيث تم إعتماد هذا النظام بتاريخ 14 أفريل لسنة 2016، ومر بفترة إنتقالية تراوحت مدتها سنتين ليصبح ساري المفعول ويُنفذ بتاريخ 25 ماي لسنة 2018، وحل محل نظام حماية البيانات الذي تم إقراره في سنة 1995[1].

وما يلاحظ أن اللائحة العامة لحماية البيانات GDPR جاءت بمبادئ ومصطلحات لا تختلف كثيرا عن تلك الواردة في توجيه عام 1995، إلا أنها أضافت مبادئ جديدة وضبطتها، حيث ضبطت مفهوم الموافقة وحددته، وحددت شروط نقل البيانات، ونصت على مبدأ الحق في النسيان، هذا ما جعل أوربا تستقطب الشركات متعددة الجنسيات، إلا أنها بالمقابل جاءت بإلتزام جديد يتمثل في الإخطار بالإنتهاكات الأمنية[2].

See information available at:
https://web.archive.org/web/20180831164911/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation /

accessed : May 10, 2023 At21 :28.

تم الإطلاع عليه بتاريخ 11/ 05/ 2022 على الساعة 21:28.

[1] موسوعة ويكيبيديا، متوفر على الرابط التالي:
https://ar.wikipedia.org/wiki/%D8%A7%D9%84%D9%86%D8%B8%D8%A7%D9%85_%D8%A7%D9%84%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D9%8A_%D8%A7%D9%84%D8%B9%D8%A7%D9%85_%D9%84%D8%AD%D9%85%D8%A7%D9%8A%D8%A9_%D8%A7%D9%84%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA

تم الإطلاع عليه يوم 22/ 05/ 2022 على الساعة 17:56.

2 W.Scott Blackmer Getting Ready for the New EU General Data Protection Regulation, 5 May, 2016 See information available at:

https://web.archive.org/web/20180831164911/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-/ getting-ready-for-the-new-eu-general-data-protection-regulation

accessed : May 11, 2023 At 21 :30.

فبموجب القانون رقم 2016/679– 27 أفريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات وتم إلغاء القانون EC/95/4.[1]

حيث تحتوي اللائحة على 99 مادة، الفصل الأول منها عُنون بأحكام عامة، حددت المادة الأولى منه الموضوع والأهداف المرجوة من هذا القانون، حيث نظم هذا القانون القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وكذلك القواعد المتعلقة بحركة البيانات الشخصية، والهدف منه حماية الحقوق والحريات الأساسية للأشخاص الطبيعيين، وعلى وجه الخصوص حقهم في حماية البيانات الشخصية، وحظر تقييد حرية نقل البيانات الشخصية داخل الإتحاد الأوربي أو منعها لأي سبب من الأسباب المتعلقة بحماية الأشخاص الطبيعيين بخصوص بمعالجة البيانات الشخصية[2].

أما المادة الثانية منه فنصت على نطاق تطبيق هذا القانون، وحددت المادة 03 النطاق الإقليمي لتطبيق هذا القانون، أما المادة 4 فقد عرفت المصطلحات التقنية والمصطلحات الغامضة التي نصت عليها هذه اللائحة كالبيانات الشخصية، المعالجة، تقييد المعالجة، المراقب، المعني، المتلقي، الطرف الثالث، البيانات الوراثية، البيانات البيومترية، البيانات المتعلقة بالصحة، السلطة الإشرافية...الخ[3].

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel de l'Union européenne.

للإطلاع على القانون رقم 679/ 2016 – 27 أفريل 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات باللغة الفرنسية متوفر على الرابط التالي:

https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN .

[2] Art 01 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[3] Articles 03 et 04 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

أما المادة 05 فإنها نصت على المبادئ المتعلقة بمعالجة البيانات الشخصية والمتمثلة في:

_ مبدأ المشروعية والإنصاف والشفافية.

_ مبدأ الغائية أي الهدف الذي جمعت من أجله هذه البيانات لغرض معالجتها

_ مبدأ تقليل البيانات وملائمتها ومحدوديتها (أي لابد أن تكون هذه المعالجة متناسبة مع الأغراض التي جُمعت لأجلها هذه البيانات كما ونوعا)

_ مبدأ دقة البيانات

_ مبدأ تحديد مدة التخزين

_ مبدأ السلامة والسرية

_ مبدأ مسؤولية المراقب[1].

أما المادة 6 فنصت على شروط شرعية أو قانونية المعالجة[2]، أما المادة 7 منه نصت على شرط الموافقة من طرف صاحب البيانات، حيث يجب على القائم بالمعالجة إثبات موافقة صاحب البيانات على معالجة بياناته الشخصية، مع وجوب وضوح تصريح الموافقة ووضوح لغته بعدم قابليتها لتأويل[3]. أما المادة 8 فنصت على الشروط المطبقة على موافقة الطفل فيما يتعلق بخدمات مجتمع المعلومات، أما المادة 9 منها فنصت على معالجة فئات خاصة من البيانات الشخصية، والمادة 10 على معالجة البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم أي بالماضي الجزائي، المادة 11 نصت عن المعالجة التي لا

[1]Art 05 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[2] Art 06 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[3] Art 07 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

تتطلب تحديد هوية[1]. أما الفصل الثالث فنص على حقوق صاحب البيانات تم تقسيمه إلى 4 أقسام، ومن هذه الحقوق حق الوصول عن طريق صاحب البيانات المادة (15)، الحق في التصحيح (المادة 16)، الحق في المسح " الحق في النسيان" المادة (17)، الحق في تقييد المعالجة (المادة 18)،الحق في قابلية نقل البيانات المادة 20، حق صاحب البيانات في الاعتراض عن معالجة بياناته (المادة 21)[2].

وحسب رأينا فإن النظام العام الأوروبي لحماية المعطيات الشخصية " **General Data Protection Regulation**" يعتبر أحسن نموذج تشريعي لحماية المعطيات الشخصية، فهو أضفى حماية شاملة للمعطيات من خلال نصه على مبادئ المعالجة وشروطها، ونصه على فئة المعطيات الحساسة، وعلى حقوق صاحب المعطيات، حيث يمكن لهذا الأخير تدارك الأخطأ التي تكون خلال المعالجة إذا ماتمت موافقته فله حق التصحيح والمسح، وحقه في تقييد المعالجة، وكذلك الإعتراض عليها.

الفرع الثاني: التشريعات المتعلقة بحماية المعطيات الشخصية على المستوى الافريقي

في البداية مهد لحماية المعطيات الشخصية الميثاق الإفريقي لحقوق الإنسان والشعوب بموجب نصت المادة 8 منه على إنتهاك حقوق الإنسان وكرس حقه في احترام حياته الشخصية[3]، ثم ظهرت تشريعات على المستوى الإفريقي لحماية المعطيات الشخصية والتي تتمثل في:

[1] les Articles 8 et 9 et 10 et 11 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[2] les Articles à 12 vers 21 de la RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[3] Art 8 RÈGLEMENT (UE) 2016/679, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

أولا: القانون المتعلق بحماية البيانات الشخصية داخل المجلس الاقتصادي والاجتماعي لمجموعة دول غرب افريقيا

ويطلق عليه كذلك قانون الجماعة الاقتصادية لدول غرب افريقيا، تم اعتماده في الدورة السابعة والثلاثين لسلطة رؤساء الدول والحكومة في أبوجا في اليوم السادس عشر بتاريخ 13 شباط/ فبراير 2010[1]. هذا القانون أضفى حماية على البيانات الشخصية لدول غرب افريقيا.

ثانيا: إتفاقية الاتحاد الافريقي بشأن أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي 2014

إن غياب سياسة جنائية واضحة وشاملة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في الدول الإفريقية، ما جعل هذه الجرائم تتزايد بشكل كبير، لا سيما تلك التي يتم استخدام الانترنت فيها ومواقع التواصل الاجتماعي، هذا حسب تقرير الأنتربول. على الرغم من أن الاتحاد الأفريقي اعتمد في سنة 2014 اتفاقية بشأن الأمن الالكتروني وحماية البيانات الشخصية ، إلا أنه إلى غاية يناير 2020، وقعت عليها 14 دولة فقط من أصل 55 دولة عضو في الاتحاد الأفريقي هذا ما جعلها غير نافذة، لأنه يجب أن يتم التصديق على هذه الاتفاقية من قِبَل ما لا يقل عن 15 دولة عضو حتى تدخل حيز التنفيذ، وحتى تاريخ يناير 2020 صادقت عليها سبع (7) دول فقط، ويتضح من ما توصل إليه التقرير أن غالبية الدول الإفريقية لا تزال لا تولي الأمن السيبراني أهمية، وتعتبره غير ضروري مما يفاقم المشكلة[2].

وما يجدر الإشارة إليه أنه يطلق عليها كذلك تسمية اتفاقية مالابو، وتعتبر اتفاقية مالابو هي أول صك دولي في إفريقيا بشأن حماية البيانات الذي تم إقراره في عام 2014،

[1] Olumide Babalola, op.cit ,P45.

[2] تقرير للإنتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أيّ وقت مضى، 14 أغسطس، 2020. أنظر الموقع الرسمي للأنتربول، متوفر على الرابط التالي: https://www.interpol.int/ar/1/1/2020/36 تم الإطلاع بتاريخ 2022/09/04 على الساعة 11:05.

ومن بين أهم أهدافها مواءمة قوانين الدول الأعضاء بشأن حماية البيانات وتشجيع الأعضاء الدول لإنشاء أطر قانونية مشتركة لحماية البيانات الشخصية داخل القارة الافريقية[1].

تضمنت هذه الاتفاقية أربعة فصول حيث أقرت حماية البيانات الشخصية بموجب الفصل الثاني منها، والذي تضمن أربعة أقسام أولها موسوم بحماية البيانات الشخصية تضمن ثلاثة مواد (من م8 إلى م10)[2]، وبين الإجراءات الأولية لمعالجة البيانات الشخصية بموجب المادة10[3]، إضافة إلى أنه تم تحديد الإطار المؤسساتي لحماية البيانات الشخصية في القسم الثاني منها الذي تضمن المادتين (11 و12) منها التان نصتا على تشكيلة وتنظيم سلطات حماية البيانات ذات الطابع الشخصي، وواجباتها وصلاحيتها[4]، ونصت كذلك على الالتزامات المتعلقة بالشروط التي تحكم معالجة البيانات الشخصية، يتكون من 3 مواد (من المادة 13 إلى المادة 15).

وهذه الاتفاقية كغيرها من الاتفاقيات المتعلقة بحماية المعطيات الشخصية نصت على المبادئ الأساسية التي تحكم معالجة البيانات الشخصية في (المادة 13) والتي تتمثل هذه المبادئ الستة للمعالجة:

_ مبدأ الموافقة وشرعية معالجة البيانات الشخصية

_ مبدأ قانونية ونزاهة معالجة البيانات الشخصية

_ مبدأ الغرض، وأهمية وتخزين البيانات الشخصية المعالجة بيانات

_ مبدأ دقة البيانات الشخصية

[1] Instrument Juridique de l'Union Africaine, convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel, Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014, document U.A N : EX.CL/846(XXV).

[2] Art 08 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

[3] Art 10 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

[4] Art 10 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

_ مبدأ الشفافية في معالجة البيانات الشخصية

_ مبدأ السرية وأمن معالجة البيانات الشخصية[1].

وحَظَرَت هذه المادة معالجة وجمع هذا النوع من البيانات كقاعدة عامة، ونصت على الإستثناءات التي لا يكون فيها حظر معالجة هذه المعطيات حصرًا بموجب المادة 14منها[2]، أما القسم الرابع منها الإتفاقية فإنه نص على الحقوق الأساسية لأصحاب البيانات ذات الطابع الشخصي والمتمثلة في الحق في المعلومات (المادة 16)، حق الوصول (المادة17)، حق الاعتراض (المادة 18)، وحق التصحيح أو المحو (المادة 19)[3]، وبالمقابل نجد القسم الخامس منها نص على التزامات المسؤول عن معالجة البيانات ذات الطابع الشخصي والمتمثلة في التزامات السرية (المادة 20)، التزامات الضمان (المادة 21)، التزامات التخزين (المادة 22)، التزامات الاستدامة (المادة 23)[4].

أما الفصل الثالث عُنون " تعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية": حيث تم تقسيمه إلى قسمين: القسم الأول: إجراءات الأمن الإلكتروني الواجب اتخاذها على المستوى الوطني وتتمثل هذه الإجراءات في: وضع إطار لتأمين الفضاء الإلكتروني الوطني بموجب (المادة 24) من خلال انتهاج سياسة وطنية لهذا الغرض، واعتماد آليات مناسبة وكافية لتنفيذ هذه السياسة، وكذلك إتخاذ تدابير وإجراءات قانونية من خلال سن نصوص تشريعية بمختلف أنواعها لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من خلال تجريم كافة الأفعال الماسة بأنظمة المعلومات وبياناتها. والنص على إجراءات متابعة ملاحقة المخالفين، وكذاك على ضرورة اعتماد تدابير تشريعية وتنظمية التي تسند المسؤولية

[1] Art 13 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

[2] Art 14 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

[3] les Articles à 16 vers 19 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

[4] les Articles à 20 vers 23 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.

إلى الأشخاص المعنوية، إضافة إلى ضرورة الموازنة بين التدابير والإجراءات القانونية المتخذة بشأن أمن الفضاء الإلكتروني، والحقوق الدستورية والحقوق المحمية بموجب الإتفاقيات الدولية[1].

إضافة إلى نصها على التعاون الدولي في المادة 28 منها[2].

أما القسم الثاني منها فوردت فيه الأحكام الجزائية، حيث حددت المادة 29 من الإتفاقية الجرائم الخاصة بتكنولوجيات الإعلام والاتصالات والمتمثلة في: الهجمات على أنظمة الكمبيوتر، خروقات البيانات المحوسبة، الجرائم ذات الصلة بالمحتوى، الجرائم المتعلقة بإجراءات تأمين الرسائل الإلكترونية[3]، وتم النص من خلالها كذلك على مواءمة بعض الجرائم إلى تكنولوجيا الإعلام والاتصال وتتمثل في جرائم الممتلكات والمسؤولية الجنائية للأشخاص الاعتباريين[4]، وتم النص من خلالها كذلك على مواءمة عقوبات معينة مع تكنولوجيا الإعلام والاتصال[5].

وما يجدر ذكره في هذا الصدد أنه في الواقع 28 دولة فقط من بين 30 دولة لديها قوانين حماية البيانات في أفريقيا لديها سلطات حماية البيانات (DPAS). وما يؤخذ على هذه الاتفاقية أنها تحتوي فقط على ستة مبادئ معاد صياغتها مبادئ الحماية مع بعض الاختلاف عن المبادئ المعترف بها عالميا[6].

وأن هذه الاتفاقية لن تكون فعالة، إلا إذا تم دعمها على الصعيد الوطني بآليات ذات مصداقية تخدم إرادة سياسية حقيقية لتعزيز أمن الفضاء السيبراني، ويتطلب ذلك جملة من

[1] Art 24 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.
[2] Art 28 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.
[3] Art 30 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.
[4] Art 30 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.
[5] Art 31 de la convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel.
[6] Olumide Babalola, POLICY BRIEF, Data Protection Legal Regime and Data Governance in Africa: An Overview, African Economic Research Consortium, Kenya, No.DG003, February 2022, p 2 – 3.
See information available at: file:///C:/Users/user/Downloads/DG003.pdf

الآليات، كإنشاء إطار قانوني لمكافحة الجريمة السيبرانية وتنفيذه تنفيذا فعالا، أوإستحداث شرطة متخصصة في هذا النوع من الجرائم، وتبني استراتيجية وطنية لأمن أنظمة المعلومات[1]، وننوه في الأخير أن هذه الاتفاقية لم تصادق عليها الجزائر.

[1] DEHBI Abdelhakim , Cybersecurity in Africa: Challenges and measures, WORLD POLITICS , Volume (6), N°(2), 2022. p1060.

الفصل الثاني: السياسة الجنائية الدولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الإجرائي

بالرغم من وجود العديد من الآليات الاتفاقية على المستوى الدولي، ووجود العديد من الجهود المبذولة من طرف المنظمات الدولية، فإن هذا غير كافٍ للتصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بل يتطلب تفعيلها تعاون دولي وتدابير وإجراءات لتطبيقها في أرض الواقع.

وحتى يتم يتفعيلها واقعيًا لابد من تطبيق قواعد الاختصاص الجنائي الدولي، وكذلك تطبيق آلية التعاون القضائي الدولي.

ولذلك سنتطرق في هذا الفصل للإختصاص القضائي الدولي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الأول)، والتعاون القضائي الدولي (المبحث الثاني).

المبحث الأول: الإختصاص القضائي الدولي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

لا تثير مسألة الاختصاص على المستوى الوطني أي مشكلة لأنه فيها يتم الرجوع إلى المعايير المعتمدة قانونا، ولكن تُثار مشكلة الاختصاص على المستوى الدولي[1]، كون الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ترتبط بشبكة المعلومات العالمية، هذا ما يؤدي إلى أن يكون إقليم أكثر من دولة مسرحا لجريمة واحدة، حيث قد ترتكب الجريمة في إقليم دولة وتتحقق نتيجة الجريمة في دولة أخرى، هذا الأمر يؤدي إلى تنازع الاختصاص بين هذه الدول، وهذا التنازع يرجع أساسا إلى إختلاف التشريعات والنظم القانونية من دولة إلى أخرى[2]، والتنازع يتخذ شكلين، تنازع إيجابي يكون بتمسك كل جهة قضائية بالنظر في القضية، وقد يكون سلبي في الحالة العكسية التي ترفض فيها كل جهة النظر في القضية.

لذا وجب علينا تحديد القانون الواجب التطبيق على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، والتطرق للإختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الثاني).

---

[1] وائل محمد نصيرات، الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية– ICACC، جامعة الإمام محمد بن سعود الإسلامية– كلية علوم الحاسب والمعلومات، الرياض، المملكة العربية السعودية، نوفمبر 2015، ص133. مقال منشور على الرابط التالي:

http://search.mandumah.com/Record/690618

تم الإطلاع بتاريخ 2022/09/08 على الساعة 11:00.

[2] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، ط1، دار الفكر الجامعي، الاسكندرية، 2020، ص78.

المطلب الأول: تحديد القانون الواجب التطبيق على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لا يحدها موقع جغرافي ثابت أو دولة معينة بل تنتشر في جميع دول العالم حيث على عكس الجرائم التقليدية الأخرى، فهي عابرة للحدود الوطنية، مما يترتب عن ذلك عدم وجود قانون جنائي محدد أو موحد يحكم هذه الجريمة بل بالعكس هناك العديد من القوانين الجنائية تتعدد وتختلف بتعدد الدول والأنظمة القانونية ويرجع ذلك أساسا إلى الصلة بين القانون الجنائي والسيادة الوطنية[1].

واستنادا على ما سبق من خلال هذا المطلب سنبين قواعد تحديد القانون الواجب التطبيق في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والمبدأ الذي يتوافق ويتلاءم مع طبيعتها الخاصة التي تنفرد بها.

الفرع الأول: المبادئ التي تحكم الإختصاص القضائي

بداية وقبل التطرق إلى المبادئ التي تحكم الإختصاص القضائي يجب علينا تعريف الاختصاص والذي هو أهلية إحدى السلطات للقيام بأعمال معينة، وفي القضاء الجزائي هو أهلية القاضي للفصل في الدعوى الجزائية وفي الدفوع المقدمة بشأنها، فالاختصاص يعني أهلية المحكمة للنظر في الدعوى، وبما أن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تعتبر جرائم عابرة للحدود الوطنية، فهي قد تقع بكاملها في دولة واحدة وقد تقع في عدة دول، لذلك فإن الاختصاص في القضاء ينقسم إلى نوعين داخلي وخارجي[2]، ويُعرف الاختصاص القضائي بأنه: "السلطة التي خولها القانون لمحكمة ما في الفصل في نزاع ما"،

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، ط1، دار الفكر الجامعي، الاسكندرية، 2020، ص98.

[2] مناصرة يوسف، المرجع السابق، ص83.

ويقصد بالاختصاص القضائي الدولي اختصاص محكمة دولة ما بنزاع يخص علاقة قانونية مشوبة بعنصر أجنبي[1].

وللاختصاص القضائي مبادئ تحكمه، ما يقتضي منا ضرورة التطرق لها كما يلي: مبدأ الإقليمية (أولا)، مبدأ الشخصية (ثانيا)، مبدأ العينية (ثالثا)، أما مبدأ العالمية والذي يعتبر مبدأ مهم في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، لذا سنفرد له مطلبا خاصا للتعمق فيه أكثر.

أولا: مبدأ الإقليمية

هذا المبدأ مستقر عليه في جميع قوانين العالم ويطلق عليه مبدأ إقليمية النص الجنائي أو مبدأ إقليمية قانون العقوبات « le principe de la territorialité du droit pénal » حيث يطبق مبدأ الإقليمية على كل جريمة وقعت على إقليم الدولة الجزائرية دون مراعاة لجنسية مرتكبها[2].

ويرتبط مبدأ الإقليمية بسيادة الدولة على إقليمها والتي تقتضي ألا يسري قانون غير قانونها الوطني على أية جريمة تقع على نطاق إقليمها (الوجه الإيجابي) هذا من جهة، ومن جهة أخرى ألا يمتد تطبيق قانونها إلى خارج حدود إقليمها (الوجه السلبي)[3].

ويثار الإشكال بخصوص مبدأ الإقليمية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات كون مجالها إقليم إفتراضي لا توجد فيه حدود معروفة، لأن الفضاء الإلكتروني هو عالم موازي للعالم المادي[1].

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص67.

[2] حنان المساوي، إثبات جريمة السرقة المعلوماتية والقانون الواجب التطبيق، مجلة الأبحاث والدراسات القانونية، المركز المغربي للدراسات والإستشارات القانونية وحل المنازعات، المغرب، العدد 4، نونبر – دجنبر، 2014، ص171.

[3] محمد حبحب، تطبيق القواعد الجزائية الإجرائية على الجريمة الإلكترونية: تحديات وآفاق، مجلة كلية القانون الكويتية العالمية، كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس، ملحق خاص، المجلد 6، العدد 3، الجزء الأول، 9- 10 مايو 2018م شعبان 1439، ص422.

فالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تعتبر من الجرائم التي يتجاوز مداها أحيانا حدود الدولة وذلك حينما ينقسم ركنها المادي ويتجزأ أو يتوزع على أكثر من مكان، حيث يقع السلوك في إقليم دولة وتتحقق النتيجة في إقليم دولة أخرى وفي هذه الحالة يثور التساؤل من أجل تحديد القانون الواجب التطبيق؟ ولتحديد القانون الواجب التطبيق لابد من تحديد مكان الجريمة أو إستحداث معايير بديلة لربط الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بإقليم واقعي محدد.

1_ تحديد مكان إرتكاب الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

توجد 3 أراء فقهية في هذا الصدد:

أ_ الرأي الأول: ذهب هذا الرأي إلى أن العبرة في تحديد مكان الجريمة بالمكان الذي وقع فيه السلوك الإجرامي بغض النظر عن المكان الذي تحققت فيه النتيجة[2]، والأثار المترتبة عليه، وهذا رجع إلى أن هذا المعيار يسهل عملية الإثبات وجمع أدلة الجريمة السيبرانية، خصوصا وأن المحكمة التي تنظر في القضية تكون قريبة من مسرح الجريمة، ويستند أصحاب هذا الرأي إلى أن تطبيق قانون الدولة التي تحقق فيها الضرر لايتفق واعتبارات العدالة لأن الجاني لا يكون على دراية بقوانين تلك الدولة التي سيتم إعمالها بحقه وتطبيقها عليه[3].

ب_ الرأي الثاني: ذهب أصحاب هذا الرأي إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي تحققت فيه النتيجة أو من المفترض تحققها فيه.

---

[1] Titouche Radia, Territorialité du droit pénal et cybercriminalité , Cahiers de Politique et de Droit , Onzième année – Vol 11 – N° 01 , Janvier 2019 ,P30.

[2] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 79.

[3] عراب مريم، الإختصاص القضائي في الجريمة المعلوماتية، حوليات كلية الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة وهران، الجزائر، المجلد 07، العدد 03، ديسمبر 2015، ص277.

ج_ الرأي الثالث: ذهب أصحاب هذا الرأي إلى أن العبرة تكون بمكان حصول أي منهما[1]، أي بمكان وقوع السلوك المجرم، أو مكان تحقق النتيجة، هذا الاتجاه لاقى قبولا من غالبية الفقه، ومبرره أن الركن المادي للجريمة يقوم على ثلاث عناصر، وهي الفعل أي النشاط الإجرامي، والنتيجة وعلاقة السببية، مما يعني أن الجريمة وقعت في كل مكان تحقق فيه عنصر من عناصر الركن المادي للجريمة[2].

وحسب رأينا فإن الرأي الثالث هو الأفضل في تحديد القانون الواجب التطبيق على الجرائم المتعلقة بانظمة المعالجة الآلية للمعطيات، حتى لا يكون هناك إفلات من العقاب للمجرمين المعلوماتين.

وما يجب الإشارة إليه أن غالبية الدول تبنت مبدأ إقليمية النص الجنائي بهدف حل مشكلة الإختصاص القضائي في الجرائم المعلوماتية بصفة عامة، إلا أن الدول اختلفت في طريقة تبني مبدأ الإقليمية كحل لمشكلة الاختصاص القضائي، فبعضها تبنى تشريعات خاصة تتعلق بالجرائم المعلوماتية، وساير البعض الأخر الإجتهاد القضائي، وبعض الدول الأخرى تبنت الحل عن طريق الاتفاقيات الدولية[3].

ويثار الإشكال بخصوص مبدأ الإقليمية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات كون مجالها إقليم إفتراضي لا توجد فيه حدود معروفة، لأن الفضاء الإلكتروني هو عالم موازي للعالم المادي[4]، وهذه الجريمة غالبا ماتكون عابرة للحدود الإقليمية للدول.

وهناك من يرى محدودية إعمال القانون الواجب التطبيق في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لأن المعطيات بمختلف أشكالها تنقسم إلى كتل لا تعبر كلها عن

[1] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 79.

[2] عراب مريم، المرجع السابق، ص 278 – 279.

[3] عراب مريم، المرجع نفسه، ص 278.

[4] Titouche Radia, OP.Cit, P30.

الطرق نفسها، وهذا نتيجة للأصل العسكري للشبكة الانترنت، وعلى الرغم من إمكانية تحديد هوية الأجهزة وأماكنها باستثناء حالات خاصة جدا.

وحتى يتم تجاوز الإشكال المرتبط بمكان ارتكاب الجريمة، يرى بعض الفقه أن الحاسب الخادم الخاص بالإيواء[1] في الخارج (أي خادم الاستضافة) لا أثر له على وقوع الجريمة على الإقليم الوطني، حيث أن الفعل الإيجابي للمستخدم هو الذي يجسد الركن المادي للجريمة، وإن كانت الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تأخذ بعدا دوليا وذلك حينما ترتكب داخل الدولة إلا أنها تمتد إلى خارج هذا الإقليم، ويمكن أن تكون هذه الجريمة وطنية، يقتصر أثرها على هذا الإقليم ولا يتجاوزه "لأن حجم الأثر المكاني يحويها كأي جريمة ثانية لكونها ينبغي أن تبدأ في نطاق إقليم معين، ومن ثم ينعقد الإختصاص الجنائي لذلك الإقليم..."[2].

ونظرا لخصوصية الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات كونها محلها الفضاء السيبراني تم إستحداث معايير بديلة لربط الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بإقليم واقعي محدد هذا ما سنتطرق إليه.

[1] الحاسب الخادم الخاص بالإيواء ويقصد به نظام المعالجة الآلية للمعطيات.

[2] حنان المساوي، المرجع السابق، ص175.

2_ إستحداث معايير بديلة لربط الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بإقليم واقعي محدد:

أ_ مكان الاتصال ونظام عنوان IP[1] (عنوان بروتوكول الأنترنت):

حتى لو كان من المستحيل تحديد مكان الجريمة المرتكبة في بيئة إفتراضية، يمكننا دائمًا ربطه بنقطة محددة من البيئة الواقعية، وذلك عند ارتكاب إحدى الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، يقوم المجرم المعلوماتي بذلك من نقطة جغرافية محددة يمكن اعتبارها مكان ارتكاب الجريمة.

ويمثل هذا المعيار البديل الذي من شأنه أن ينقل مبدأ الإقليمية من الجرائم التقليدية إلى الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات، وبالتالي، يبدو أن عنوان بروتوكول الانترنت "IP address" فعالة كونها الأكثر ارتباطًا بضحية الجريمة، ومزودو خدمة الوصول هم من يخصصون عنوان IP لعملائهم وتتصل هذه الأخيرة بالإنترنت، يظهر بروتوكول الإنترنت أو عنوان IP كمفهوم للمزية التقنية والقانونية على حد سواء، ولكنها ذات أهمية كبيرة بالنسبة للمستخدم، وهو سبب إلزام المشرع الجزائري مزودو خدمات الإنترنت للاحتفاظ ببيانات حركة المرور من زبائنها، ولا سيما تلك المتعلقة بالبيانات التي تمكن من تحديد مستخدمي الخدمة بالإضافة إلى الالتزام بإبلاغهم إلى السلطات المختصة، على سبيل المثال، مكان إصدار المواقع المستخدمة في الجريمة التي قد تتوافق مع المنزل هو معيار

[1] Adresse IP (lP Address) :" C'est une adresse numérique, identifiant chaque ordinateur sur l'arborescence du réseau Internet. Cette adresse est composée de 4 nombres compris entre 0 et 255 . Ces nombres sont séparés par 3 points.
Exemple: 123.124.213 .122, désigne la 122 éme machine située sur le 213éme sous-réseau du sous-réseau 124 qui se trouve sur le réseau global 123. Les adresses IP sont soit routables, soit non-routables.
Les adresses routables peuvent être utilisées à travers tout l'Internet alors que les non-routables ne seront pas pris en charges par les routeurs. Les adresses non-routables sont en général utilisées derrière les pare-feux. Il existe uniquement trois étendues d'adresses non-routables, Toutes les autres adresses sont routables et doivent être uniques sur Internet., ce qui signifie que si votre foumisseur d'accès Internet (FA!) vous attribue par exemple l'adresse 68.11.31.26, aucune autre machine ne doit avoir l'adresse 68.11.31.26 dans le monde."
أنظر: قاموس المصطلحات المستعملة في الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، وزارة العدل، الجزائر.

يمكن استخدامه، وكذلك الموقع الخادم الذي يحمل الموقع المستخدم في الجريمة. وتنطبق المادة 586 من قانون الإجراءات الجزائية الجزائري[1] على هذه المسألة فقط.

ب_ ظهور نظرية إمكانية الوصول إلى الموقع أو المحتوى:

وفقا لهذه النظرية، فإن إمكانية الوصول إلى المحتوى غير المشروع من الأراضي الجزائرية تشكل العنصر المكون للجريمة، الذي يستدعي اختصاص القانون الجنائي الجزائري بغض النظر عن مصدره.

هذا ما اعتمده القضاء الفرنسي والذي اعتبر أن الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات مُرتكبة على الأراضي الفرنسية بمجرد الوصول إلى المحتوى غير المشروع والمعلومات في فرنسا. وفي هذا الصدد وبموجب حكم مؤرخ 26 شباط/فبراير 2002، أشارت المحكمة العليا في باريس (الدائرة السابعة عشرة) إلى أن "القاضي الفرنسي مختص في مدى إمكانية الوصول إلى رسائل أو محتوى الموقع عن طريق الإنترنت، على الأراضي الفرنسية "، حيث اعتبرت أنه يشكل الإقليم الفرنسي بالفعل عنصرا من عناصر الجريمة المنصوص عليها في المادة 113- 2 من قانون العقوبات الفرنسي[2].

وكذلك بالنسبة " لقضية ياهو yahoo " التي صدر بشأنها اجتهاد قضائي فرنسي والتي منحت الاختصاص القضائي للقاضي الفرنسي بمجرد إمكانية الوصول للموقع من فرنسا[3].

وحسنا فعل المشرع الفرنسي بربط تطبيق مبدأ الإقليمية بإمكانية الوصول للمحتوى على الاقليم الفرنسي، وهو توجه نحو توسيع مصطلح الاقليمية، والحديث عن الإقليم السيبراني أو الرقمي للدولة، وتجسيد السيادة السيبرانية للدول على إقليمها السيبراني، وهذا توجه جديد ينادي به فقهاء القانون الدولي.

[1] تنص المادة 586 ق.إ.ج.ج على أنه: " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر"

[2] Titouche Radia, Op.Cit, p 31 - 32.

[3] Romain BOOS, Op.Cit , p167.

ج- نظرية التركيز:

حيث تغيرت وجهت نظر الفقه الفرنسي من نظرية إمكانية الوصول إلى الموقع أو المحتوى[1]، إلى نظرية التركيز والتي تتطلب إستهداف المحتوى غير المشروع أو المعطيات غير المشروعة أو موقع الأنترنت الجمهور الفرنسي ويكون بِلُغَتِهِ (اللغة الفرنسية)، وبالتالي فالمحتوى الذي لا يمكن الوصول اليه من فرنسا وكُتِب بِلُغَةٍ غَيْرِ اللُّغَةِ الفرنسية يعتبر موجها لجمهور أخر، وبالتالي فرنسا تعتبر غير مختصة إقليميا.

لذا اتجه الفقه نحوى تقييد مجال إختصاص القضاء الفرنسي الإقليمي باعتماد هذه النظرية الجديدة حيث رأى الفقه الفرنسي أنه من الضروري وضع معايير جديدة للحد بشكل معقول من الاختصاص الإقليمي لدولة ما في مواجهة حالة يمكن فيها للجميع المطالبة باختصاصهم على قدم المساواة، وهذه النظرية أنشأها القضاء الامريكي[2].

وما يجدر بنا الإشارة اليه أن المشرع الجزائري لم يساير الاتجاهات الفقهية الحديثة، بل اكتفى بتبنيه لمبدأ الإقليمية بالمفهوم التقليدي لتحديد الاختصاص المكاني، ووفقا للقواعد التقليدية المحددة لمعايير الاختصاص الاقليمي الذي نصت عليه المادة 03 من قانون العقوبات[3]، والمادة 586 من قانون الإجراءات الجزائية الجزائري[4].

[1] حسب نظرية إمكانية الوصول إلى الموقع أو المحتوى يمكن لأي دولة تصل لهذا المحتوى أن تكون صاحبة الاختصاص الإقليمي وهذا يثير مشكلة تنازع الاختصاص.

[2] Romain BOOS, Op.Cit , P174 - 378.

[3] تنص المادة 03 من ق ع " يطبق قانون العقوبات الجزائري على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق أيضا على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم الجزائرية طبقا لقانون الإجراءات الجزائية".

[4] تنص المادة 586 من ق إ ج " تعتبر الجرائم مرتكبة في الاقليم الجزائري كل جريمة يكون عملا من الأعمال المميزة لأحد أركانها قد تم بالجزائر".

ثانيا: مبدأ الشخصية

ويقصد بهذا المبدأ أن المواطن، أينما كان، يمكن أن يخضع لقانون بلده، فإذا ارتكب مواطن جريمة في الخارج وعاد إلى بلده قبل محاكمته عليها، وقبل أن يقضي العقوبة المحكوم بها عليه، فإنه يجوز متابعته ومحاكمته في بلده الأصلي[1]، وينقسم إلى:

1_ مبدأ الشخصية الإيجابي:

يعتبر مبدأ الشخصية الإيجابية وسيلة لمنع الجاني من الإفلات من العقاب وذلك في حالة ما إذا ارتكب جريمة خارج بلده ثم عاد إليه، ففي هذه الحالة لا يمكن للدولة وفقا لمبدأ الإقليمية معاقبته لأن الجريمة لم ترتكب على أراضيها، ولا يمكنها كذلك تسليمه لأن الدولة لا تسلم مواطنيها ورعاياها، كما أن الدولة التي تم ارتكاب الجريمة على أراضيها لن تستطيع معاقبة الجاني إذا غادرها بعد ارتكابه للفعل المُجَرم، لذلك لا سبيل لتلافي الثغرات الواردة في النظام الجزائي العقابي إلا بمعاقبة الجاني عند رجوعه لأرض وطنه حتى يتم ردعه[2].

2_ مبدأ الشخصية السلبي:

لم يأخذ به المشرع الجزائري، كون هذا المبدأ يتعارض وفكرة السيادة، إلا أن نص المادة 591[3] من ق.إ.ج في الفقرة الثانية أورد صورة يمكن تصنيفها ضمن مبدأ شخصية

[1] عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول " الجريمة"، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 2009، ص111.

[2] خلفي عبد الرحمان، عثماني بلال، حماية الرعايا الجزائريين بالخارج في إطار القانون الجنائي الوطني، مجلة الدراسات حول فعلية القاعدة القانونية، مخبر البحث حول فعلية القاعدة القانونية، جامعة عبد الرحمان ميرة بجاية، الجزائر، المجلد 03، العدد01، 2019، ص 222- 223.

[3] المادة 591 من ق.إ.ج.ج : " تختص الجهات القضائية الجزائرية بنظر الجنايات والجنح التي ترتكب على متن طائرات أجنبية أيا كانت جنسية مرتكب الجريمة

كما أنها تختص أيضا بنظر الجنايات أو الجنح التي ترتكب على متن طائرات أجنبية إذا كان الجاني أو المجني عليه جزائري الجنسية أو إذا هبطت الطائرة بالجزائر بعد وقوع الجناية أو الجنحة.

القاعدة الجنائية في شقها السلبي وهي تتعلق بالجنايات والجنح المرتكبة ضد جزائريين على متن طائرات أجنبية[1]، وعليه فالمشرع الجزائري لم يتضمن ما يبين تطبيق قانونها على الجنايات والجنح باستثناء ما جاء في نص المادة السالفة الذكر، وتطبيق هذا الحكم يبقى معلقا على القبض على الجاني في الجزائر أو تسليمه وفق إجراءات التسليم، وعليه المشرع لم يأخذ بمبدأ الشخصية السلبية كونه منتقد من غالبية الفقه الجنائي لما ينطوي عليه من عدم الثقة في قضاء الدولة التي وقعت فيها الجريمة[2].

وما يجدر بنا الاشارة إليه هنا أن المشرع الجزائري في البداية لم يأخذ بمبدأ الشخصية على إطلاقه، وإنما أخذ فقط بمبدأ الشخصية الإيجابية[3]، ولكنه وتماشيا والتوجهات الجديدة أخذ به المشرع الجزائري بعد تعديل قانون الإجراءات الجزائية في سنة 2015 بموجب الأمر 15-02 في المادة 588 منه التي نصت صراحة أنه "تجوز متابعة ومحاكمة كل أجنبي ارتكب جريمة خارج الإقليم الجزائري ....أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري"[4]، لأنه قبل تعديل هذه المادة كانت تنص فقط على مبدأ العينية الذي سنتطرق إليه في المقام الموالي.

وتختص بنظرها المحاكم التي وقع بدائرتها هبوط الطائرة وفي حالة القبض على الجاني وقت هبوطها أو مكان القبض على الجاني في حالة ما إذا كان مرتكب الجريمة قد قبض عليه بالجزائر فيما بعد."

[1] عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام، د.ط، موفم للنشر، الجزائر، 2011، ص 154.

[2] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط14، دار هومه، الجزائر، 2014، ص 110- 111.

[3] عبد المجيد لخذاري، الجريمة العالمية الإرهاب نموذجا، ط1، الماهر للطباعة والنشر، سطيف، الجزائر، 2020، ص14.

[4] المادة 588 من الأمر 15-02 المؤرخ في 07 شوال عام 1436 الموافق 23 يوليو سنة 2015، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج العدد 40، االمؤرخة في 7 شوال عام 1436 الموافق 23 يوليو سنة 2015. والتي تنص" **تجوز متابعة ومحاكمة كل أجنبي، وفقا لأحكام القانون الجزائري، ارتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك** في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية أو القنصلية الجزائرية أو أعوانها، أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو **أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري**".

ثالثا: مبدأ العينية

هذا المبدأ يسمح للدولة بممارسة الاختصاص القضائي عندما يهدد فعل يقع خارج حدودها أمنها أو الوظائف الأساسية لها[1]، وكذلك المحلات الدبلوماسية والقنصلية والنقود والأوراق المصرفية المتداولة قانونا، ويكون هذا الفعل يشكل جنحة أو جناية.

قبل تعديل قانون الإجراءات الجزائية بموجب الأمر 15-02 كانت المادة 588[2] من ق. إ.ج تشترط شرطين لتطبيق هذا المبدأ وهما إلقاء القبض على الجاني في الجزائر أو أن يتم تسليمه إلى الجزائر وفقا لإجراء تسليم المجرمين، لكن بعد التعديل الذي أوردناه لقانون الإجراءات الجزائية تم التخلي عن هذين الشرطين[3].

والمبدأ الرابع هو مبدأ العالمية والذي سنفصل فيه في المطلب الثاني.

الفرع الثاني: تنظيم الإختصاص القضائي الدولي في القانون الدولي والقوانين الداخلية

حتى لا تُترك مسألة الاختصاص لاجتهاد الفقه والقضاء، لابد من تحديد موقف القانون الدولي من خلال الاتفاقيات الدولية والإقليمية[4]، وكذلك ايضاح موقف التشريعات الوطنية.

[1] Susan W. Brenner , Bert-Jaap Koops, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol IV No 1, 2004, P26.

[2] كانت تنص المادة 588 ق. إ.ج.ج قبل التعديل " كل أجنبي ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا بالجزائر تجوز متابعته ومحاكمته وفقا لأحكام القانون الجزائري إذا ألقي القبض عليه في الجزائر أو حصلت الحكومة على تسليمه لها"

[3] أنظر المادة 588 من الأمر 15-02 المتضمن قانون الإجراءات الجزائية.

[4] خليفي محمد، إشكالية الإختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، مخبر الجرائم العابرة للحدود، معهد الحقوق والعلوم السياسية، المركز الجامعي صالح أحمد بالنعامة، الجزائر، العدد1، ديسمبر 2016 ص258.

أولا: على مستوى الاتفاقيات الدولية الخاصة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

وفقًا لفكرة تحقيق الموازنة بين حق الدولة في ممارسة اختصاصها، وللتغلب على هذه المشكلة، اقترحت بعض الاتفاقيات حلاً وسيطًا يجسد إدراك الأطراف المشاركة في إبرام الاتفاقيات، مراعية البعد الدولي للجرائم المتعلقة بالمعالجة الآلية للمعطيات، ومنع إفلات المجرمين من العقاب، وذلك من أجل تجنب تداخل الاختصاص[1].

1_ اتفاقية مجلس أوروبا لمكافحة الجريمة المعلوماتية (اتفاقية بودابست): نصت هذه الاتفاقية على مسألة الاختصاص في مادتها 22 التي نصت على أنه "يعتمد كل طرف ما يلزم من تدابير تشريعية، وذلك لإقرار الاختصاص بشأن أي جريمة معلوماتية وذلك عندما ترتكب الجريمة:

_ "في إقليمه"، يطبق مبدأ الإقليمية

_ "من جانب أحد مواطنيه إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي أوجب القانون الجنائي مكان ارتكابها أو حالة ارتكاب الجريمة خارج الاختصاص القضائي الإقليمي لأي دولة".

فهذه الاتفاقية لا تستبعد أي اختصاص جنائي يمارسه أحد الأطراف وفقا لقانونه الوطني، وفي حالة مطالبة أكثر من طرف من الأطراف بالاختصاص القضائي بشأن أي جريمة معلوماتية تقررها هذه الاتفاقية، يقوم الأطراف متى كان ذلك مُلائمًا بالتشاور لغرض تحديد الاختصاص القضائي الأكثر ملائمة للمحاكمة[2].

[1] محمد محمود سعيد، جرائم غسل الأموال أحكامها الموضوعية وإجراءات ملاحقتها، ط1، دار الفكر العربي، القاهرة، 2007، ص87.

[2] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، 83.

تم إقرار هذا البند حتى لا يفلت أي مجرم معلوماتي من العقاب نتيجة الخلافات التي قد تنشب بين الدول بخصوص من لها أحقية متابعة الجاني المعلوماتي حيث تتفق الدول الأطراف في اتفاقية بودابست على دولة يتحقق فيها شرط الأفضلية في ممارسة الاختصاص القضائي على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة والجرائم المعلوماتية بصفة عامة، وهو ما يسميه بعض الفقه الاختصاص طبقا للكفاءة الافتراضية (competence sur un hypothetique) نسبة للفضاء الافتراضي الذي ترتكب فيه هذه الجريمة[1].

وهذا بغرض منح الاختصاص للجهة القضائية

2_ القانون العربي النموذجي لمكافحة جرائم الكمبيوتر:

القانون العربي النموذجي أو قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، أخذ بمبدأ إقليمية النص الجنائي في تحديد القانون الواجب التطبيق بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات[2]، وذلك وفقا لنص المادة 22 منه[3].

حيث أن هذا القانون صادق عليه مجلس وزراء العدل العرب في 2003/10/08

اعتمد هذا القانون في مجال الاختصاص على مبدأ العينية وفقا للمادة 26 والتي نصت على أنه "تسري أحكام هذا القانون على أيا من الجرائم المنصوص عليها فيه ولو

[1] جمال زين العابدين أمين أحمد، الإختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية " دراسة مقارنة"، مجلة مستقبل العلوم الإجتماعية، العدد الرابع، يناير 2021، ص 88- 89.

[2] حنان المساوي، المرجع السابق، ص172.

[3] نصت المادة 22 من القانون العربي النموذجي لمكافحة جرائم الكمبيوتر على ما يلي: " تسري أحكام التشريع الجنائي للدولة على الجريمة المعلوماتية، إذا إرتكبت كليا أو جزئيا داخل حدودها وفقا لمبدأ الإقليمية، كما تختص المحاكم فيها بالنظر للدعوى المترتبة على تلك الجرائم، وعلى الدول العربية عقد إتفاقيات لتبني المعيار الأول في حالة تنازع الإختصاص بين الدول. كما يسري التشريع الجنائي للدولة على الجرائم المعلوماتية التي تقع خارج الحدود، إذا كانت مخلة بأمنها وفقا للقواعد العامة المنصوص عليها في قانون العقوبات".

ارتكبت كليا أو جزئيا خارج إقليم الدولة متى أضرت بإحدى مصالحها ويختص القضاء الوطني بنظر الدعاوى المترتبة".

فمن خلال هذا النص يتضح أن القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية أخذ كذلك بمبدأ العينية الذي أساسه المصلحة الوطنية والتي تعتبر معيار أساسي لثبوت الاختصاص وبالتالي يتم تطبيق القانون الجنائي الوطني[1].

3_ الإتفاقية العربية لمكافحة جرائم تقنية المعلومات:

نصت المادة 30 من هذه الاتفاقية على الإختصاص كما يلي:

" 1- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت:

أ- في إقليم الدولة الطرف

ب- على متن سفينة تحمل علم الدولة الطرف

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف

د- من قبل مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان إرتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص125.

يكون فيها الجاني المزعوم حاضرا في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف أخر بناء على جنسيته بعد طلب التسليم.

3- إذا دعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم".

ومنه يلاحظ أن هذه المادة أشارت إلى المبادئ التي يجب على الدول الأطراف اعتمادها، لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها، في الفصل الثاني، وهذه المبادئ تتمثل في المبادئ التي سبق التعرض إليها، فالفقرة1 من المادة السالفة الذكر في البند أ، ب، ج نصت على مبدأ الإقليمية

أما الفقرة 1 من نفس المادة في البند د نصت على مبدأ الشخصية

أما الفقرة 1 من نفس المادة في البند هـ نصت على مبدأ العينية

أما الفقرة 2 من نفس المادة نصت على مبدأ الاختصاص العالمي

وأشارت نفس المادة إلى مشكلة تنازع الاختصاص وذلك في الحالة التي تدعي فيها أكثر من دولة طرف في الاتفاقية اختصاصها بالنظر في الجرائم الواردة في هذه الاتفاقية[1]، حيث تكون صاحبة الاختصاص الدولة التي أخلت الجريمة بأمنها أو بمصالحها، ثم تكون صاحبة الاختصاص الدولة التي وقعت الجريمة في إقليمها، ثم الدولة التي يكون الشخص

[1] وردة شرف الدين، التعاون القضائي والقانوني لمكافحة جريمة غسيل الأموال والمرتكبة بواسطة تقنية المعلومات وفقا للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، عدد خاص بأشغال الملتقى الدولي حول: آليات مكافحة جرائم الفساد في التشريعات المغاربية، منعقد بتاريخ 04/ 05 ديسمبر 2018، منشور بمجلة الباحث للدراسات الأكاديمية، المجلد 08، العدد 02، 2021، ص645- 646.

المطلوب من رعاياها وإذا اجتمعت مختلف هذه الظروف فيؤول الاختصاص إلى الدولة الأسبق في طلب التسليم[1].

والسؤال الذي يُطرح في هذا الصدد، هو من هي الدولة التي يؤول لها الاختصاص إذا تضررت أكثر من دولة جراء ارتكاب جرائم متعلقة بأنظمة المعالجة الآلية للمعطيات، حيث كما قولنا سابقا أن هذه الاتفاقية أعطت للدولة التي تضررت حق متابعة الجناة المعلوماتيين، ففي هذا الصدد تصدى الفقه الجنائي لهذه المسألة والذي استند إلى معياريين أساسيين وهما:

_ المعيار الأول: القانون الأكثر ملائمة

حيث حسب هذا الاتجاه فإنه يُنظر إلى حجم الضرر الناجم عن الجريمة المعلوماتية، وبالتالي إذا شملت هذه الأضرار أكثر من دولة فإنه يتم النظر للتفاوت الحاصل بين جميع تلك الدول المتضررة من هذه الجريمة، ويؤول في هذه الحالة الاختصاص للدولة الأكثر تضررًا، وما يؤخذ على معيار القانون الأكثر ملائمة هو محدوديته لأنه قد تكون هناك حالات تتساوى فيها الأضرار لدى أكثر من دولة.

_ المعيار الثاني: معيار الضرر المرتقب

ويتمثل في الضرر الناتج عن الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات المرتكبة عبر الأنترنت، حيث يمكن حدوثه في أي دولة مرتبطة بالأنترنت، وعليه يمكن تضرر أكثر من دولة بنفس المستوى، وعليه يستحيل تطبيق جميع قوانين الدول المتضررة على هذه الواقعة، ففي هذه الحالة يؤول الاختصاص إلى محاكم الدول التي ارتكبت فيها الجريمة المعلوماتية، فيتم تطبيق معيار الارتقاب[2].

[1] أنظر الفقرة 2 من المادة 30 الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[2] جمال زين العابدين أمين أحمد، المرجع السابق، ص90 – 91.

ثانيا: على مستوى القانون الداخلي

بخصوص الجرائم العالمية أو الجرائم العابرة للحدود الوطنية، والتي لا يمكن حصر عناصر ركنها المادي في إقليم دولة واحدة، كونها ترتبط بإقليم العديد من الدول، فإن القانون الجنائي الدولي والذي يعتبر الفرع الخارجي من القانون الوطني فإنه يكتفي في مثل هذه الحالة بالإحالة إلى القوانين الجنائية الوطنية ذات الصلة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والتي تحدد نطاق تطبيقها الإقليمي، وهذه القوانين الجنائية الوطنية تكتفي بالفصل في ما إذا كانت مختصة أم لا بحكم واقعة معينة من دون أن تهتم – في ظل غياب قانون أجنبي– إذا كان هذا القانون قابل للتطبيق، أو كان تطبيقه أكثر ملائمة أو مشروعية من تطبيق القانون الجنائي الوطني[1].

والمشرع الجزائري أخذ بالقواعد المنصوص عليها في قانون الإجراءات الجزائية في مسألة الاختصاص إذا ما تعلق الأمر بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، إضافة إلى ذلك تختصص المحاكم الجزائرية إذا كانت هذه الجرائم مرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا أو تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، هذا ما نصت عليه المادة 15 من القانون09-04 "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا أو تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"[2].

[1] العنكبي نزار، نحو قانون جنائي دولي لجرائم المعلوماتية والأنترنت ذات الصفة الدولية، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والراسات الاستراتيجية، المجلد 3، العدد 5، حزيران– كانون الثاني 2013، ص65.

[2] المادة 15 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطلب الثاني: الاختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

قبل التطرق إلى مبدأ الاختصاص العالمي لابد من التطرق إلى تعريف الجرائم العالمية التي يُطبق عليها هذا النوع من الاختصاص الجنائي ونميزها عن غيرها من الجرائم (الجريمة الدولية والجريمة الوطنية)، ونُحدد طبيعة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي هي موضوع دراستنا.

حيث ينصرف مصطلح الجريمة العالمية للدلالة على فئة من الجرائم يتم إرتكابها على نطاق عالمي واسع، فأصبحت محلا لتجريم كافة التشريعات الجنائية العالمية، ومحط عناية القانون الدولي العام فيما تم إبرامه من اتفاقيات دولية تتعلق بها، بغية تعزيز التعاون الدولي لمكافحتها وتوحيد أو تنسيق نصوص التشريعات الجنائية الوطنية بصددها، وما يجدر بنا ذكره أن الصفة العالمية لهذا النوع من الجرائم لا تغير من حيث المبدأ من طبيعتها كجرائم عادية من جرائم القانون الجنائي الداخلي، لكنها جرائم عادية من نوع خاص (suis generis) نظرا لامكانية إرتكابها في أقاليم عدة دول من قبل مجرمين من جنسيات مختلفة، ومن هنا تتأتى لها الصفة العالمية[1].

وتختلف الجريمة العالمية عن الجريمة العادية الداخلية من حيث خضوع الجرائم الداخلية حصرا إلى إختصاص القضاء الوطني للدولة التي ترتكب الجريمة على إقليمها.

تُعَرَّف الجريمة العالمية بأنها "جريمة داخلية ينص عليها القانون الداخلي وتتعاون الدول على مكافحتها عن طريق الإتفاقيات الدولية، التي تخضع للشروط التي ينتهجها قانون

[1] العنكبي نزار، المرجع السابق، ص47- 48.

العقوبات الداخلي في العقاب على تلك الجرائم، كما تنص على خضوع المجرمين لقواعد معينة متحدة في ميدان التعاون الدولي، وتكفل عقابا أكثر ملاءمة لتلك الجرائم الداخلية"[1].

في حين أن الجريمة العالمية يمكن أن تخضع إلى مبدأ الاختصاص العالمي للقضاء الجنائي الوطني، الذي يتيح لمحاكم أي دولة أن تطبق عليها ما تطبقه من أحكام القانون الجنائي الوطني المتعلق بمرتكبي الجرائم العالمية، أي كانت جنسيتهم وبصرف النظر عن مكان وقوع الجريمة لهذا بات من الأوفق القول بأن هذا النوع من الجرائم يدخل في نطاق فرع جديد من فروع القانون الجنائي هو القانون الجنائي العالمي (droit pénal universel)[2].

وتختلف الجريمة العالمية عن الجريمة الدولية حيث الجريمة الدولية يتوافر فيها العنصر الدولي وتمس بالنظام العام الدولي في حين أن الجريمة العالمية تمس بالنظام العام الداخلي ويؤول الاختصاص فيها بتقرير العقوبة المناسبة وتحديد أركانها إلى قانون العقوبات الوطني، أما الجرائم الدولية فيحدد الأركان المتوفرة فيها وعقوباتها القانون الدولي الجنائي[3].

ما يجدر الإشارة إليه أنه بالرغم من توافر الصفة الدولية في الجرائم العالمية والمتمثلة في إرتكاب الجريمة في أكثر من دولة وتعدد الجناة وإختلاف جنسياتهم واختلاف جنسيات المعتدى عليهم، إلا أنها لا تُصنف ضمن الجرائم الدولية، فالجريمة العالمية تظل جريمة داخلية وهي جرائم أفراد لا جرائم دول، بالرغم من وجود اتجاه فقهي يرى أن الجريمة العالمية جريمة دولية لأنها اعتداء على قواعد القانون الجنائي المفروضة دوليا[4].

---

[1] أميمة خديجة حميدي، إمكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة بسكرة، الجزائر، المجلد 10، العدد 01، 2022، ص1921.

[2] العنكبي نزار، المرجع السابق، ص48.

[3] سي ناصر محمد، التعاون الجزائري الدولي في مجال مكافحة الجريمة الدولية والجريمة المنظمة وتعقب المذنبين، أطروحة لنيل شهادة الدكتوراه في حقوق الإنسان والحريات، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عمار ثليجي الأغواط، الجزائر، 2021– 2022، ص 31.

[4] ابراهيم بن سليمان الحربي، الجريمة الدولية بين القانون الداخلي والقانون الوطني، دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، المجلد 6، العدد 14، مارس (آذار) 2014، ص92.

فالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يمكن أن تتخذ شكل الجريمة العالمية العابرة للحدود الوطنية، ويمكن كذلك أن تتخذ شكل الجريمة الوطنية إذا كانت لا تتعدى أثارها إقليم الدولة المرتكبة فيها ويكون مرتكبها ليس أجنبي والضحية كذلك.

الفرع الأول: مفهوم مبدأ الإختصاص الجنائي العالمي

ويطلق عليه البعض تسمية مبدأ عالمية النص الجنائي، أو مبدأ العالمية أو مبدأ الولاية الجنائية العالمية.

دعت بعض الدول إلى تطبيق هذا المبدأ في عدد ونوع محدد من الجرائم التي تعتبر عالمية الولاية القضائية، ومن الدول التي طالبت بالولاية القضائية العالمية على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بلجيكيا وألمانيا، لاسيما في جرائم نشر المواد الإباحية للأطفال على نطاق عالمي يستوجب تطبيق الولاية القضائية العالمية[1].

ومن خلال هذا المطلب سنحدد تعريف مبدأ الاختصاص العالمي (أولا)، وشروط إعمال مبدأ الاختصاص العالمي (ثانيا).

أولا: تعريف مبدأ الاختصاص الجنائي العالمي

ويقصد به تطبيق القانون الجنائي للدولة على كل جريمة يقبض على مرتكبها في إقليم الدولة أيا كان الإقليم الذي إرتكبت فيه وأيا كانت جنسية مرتكبها، بشرط القبض على الجاني في إقليم الدولة[2]، أي أن يكون لكل دولة ولاية القضاء في أية جريمة بصرف النظر عن مكان وقوعها أو مساسها بمصالحها أو جنسية مرتكبها أو المجني عليه فيها[3].

[1] Susan W. Brenner , Bert-Jaap Koops, Op .Cit, P28.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 169.

[3] أحسن بوسقيعة، الوجيز في شرح القانون الجزائي العام، المرجع السابق، ص 111.

فمن خلال تطبيقه تختص الدولة بتطبيق قانونها الجنائي على أجنبي ارتكب جريمة في الخارج وتم توقيفه أو إلقاء القبض عليه بأراضيها[1].

وما يمتاز به هذا المبدأ بأنه يقرر للقانون الجنائي نطاقا متسعا يكاد يمتد إلى العالم بأسره، فهذا المبدأ لا يجعل لمكان مرتكب الجريمة أو لجنسيته اعتبارا، ولا يشترط فيه أن يقبض على الجاني في إقليم الدولة حتى يخضع لقانونها، وهذا المبدأ اتبعته قوانين العقوبات الحديثة في الجرائم ذات الطبيعة العالمية بالنظر لخطورتها، وذلك بغرض تحقيق التعاون بين الدول فيما بينها، وما يُلاحظ على هذا المبدأ أنه يتلائم كثيرا وطبيعة الجريمة المعلوماتية رغم ما يطرحه من تنازع حاد بين التشريعات الجنائية في الدول[2].

مصدر هذا المبدأ القانون الوطني، وبذلك يختلف عن الاختصاص الدولي الجنائي الذي يعتبر مصدره القانون الدولي والذي يطلق عليه كذلك مبدأ القضاء الجنائي الدولي[3]، والذي تمارسه المحاكم الجنائية الدولية[4].

مبدأ الولاية القضائية الجنائية العالمية ترجع أصوله إلى القانون الوطني، وبالتالي فهو يتميز عن الولاية القضائية الجنائية الدولية، التي ترجع أصوله إلى القانون الدولي.

ومن خصائص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أنها تتميز بصفة العالمية أي أنها جرائم عالمية عابرة للحدود الوطنية[5]، وسُمية بالجرائم العالمية لأن مزاولة النشاط الإجرامي فيها يكون على مستوى عالمي عابر للحدود الوطنية، وبسبب طابعها العالمي العابر للحدود الوطنية ترتب عدة نتائج أهمها: ضعف فرص اكتشافها ومحاكمة

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 80.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع نفسه، ص 169-170.

[3] قطاوي أمال، نطاق تطبيق مبدأ الإختصاص الجنائي العالمي، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد إبن باديس مستغانم، الجزائر، نوقشت بتاريخ 2021/03/09 ص31.

[4] خلافي سفيان، مفهوم الولاية العالمية للمحاكم الجنائية الوطنية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، العدد2، 2012، ص 277.

[5] الطيب بلواضح، المرجع السابق، ص 191.

مرتكبيها، وصعوبة إقامة الدعوى على تلك الجرائم في ظل القوانين الحالية، إذ تصطدم بمبدأ سيادة الدولة على إقليمها[1]، وبالتالي هذا يتطلب الخروج على مبدأ الإقليمية والتخفيف من غلوه وتطبيق مبدأ عالمية حق العقاب بصددها، لمواجهة عالمية وخطورة الأضرار المتولدة عنها[2].

مما فرض بالضرورة التوجه نحو تكريس مبدأ عالمية النص الجنائي، لأنه غالبا ما يكون هنالك عجز في القوانين الداخلية التي تتصدى لهذا النوع المستحدث من الاجرام[3].

ثانيا: شروط إعمال مبدأ الاختصاص الجنائي العالمي

حتى يتم إنفاذ مبدأ الاختصاص العالمي في دولة ما لابد من توافر الشروط التالية:

1_ **النص عليه في التشريع الوطني للدولة:** التشريعات التي أخذت بهذا المبدأ نصت على الأخذ به في قوانينها من خلال:

أ_ المنهج الأول: النص في القانون الوطني على مبدأ الاختصاص الجنائي العالمي

لأن المعاهدة الدولية التي صادقت عليها الدولة والتي تعترف بمبدأ الإختصاص الجنائي العالمي لن يكون لها تأثير في مواجهة القضاء الوطني إلا إذا أصدر المشرع قانونًا ينص صراحة على تنفيذه، وذلك بإحدى الطريقتين التاليتين: الطريقة الأولى من خلال سن تشريع وطني خاص بالاتفاقية المصادق عليها والتي تنص على إدراج الجرائم المنصوص عليها في المعاهدة في القانون الوطني، وفي نفس الوقت تنص على الأخذ بمبدأ الإختصاص الجنائي العالمي، والطريقة الثانية تكون من خلال النص على مبدأ الإختصاص

[1] أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها دراسة تحليلية تأصيلية مقارنة، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص74.

[2] العنكبي نزار، المرجع السابق، ص48.

[3] الطيب بلواضح، المرجع السابق، ص 191.

الجنائي العالمي في قانون قائم مثل قانون الإجراءات الجزائية أو قانون العقوبات أو قانون العقوبات العسكري وذلك بعد المصادقة على المعاهدة ونشرها في الجريدة الرسمية[1].

ب_ المنهج الثاني: التطبيق التلقائي لمبدأ الإختصاص الجنائي العالمي الوارد في المعاهدات الدولية

يرتبط التطبيق المباشر لقواعد القانون الدولي في القانون الوطني بقاعدة سُموّ المعاهدة على القانون، وتسري الاتفاقية بمجرد تصديق الدولة عليها ونشرها في الجريدة الرسمية.

ففي هذه الحالة تُطبق نصوص الاتفاقية مباشرة في النظام القانوني للدولة، وذلك بعد إتخاذ الإجراءات القانونية التي تقرر نفاذها دون الحاجة لإصدار نص قانوني يقر بتطبيق بمبدأ الإختصاص الجنائي العالمي عند التصديق على كل إتفاقية على حده. حيث يكون كافياً للدولة أن تصادق على الاتفاقات التي تتضمن مبدأ الإختصاص الجنائي العالمي حينها يكون القاضي الوطني مختصاً بالنظر وفقاً لمبدأ الإختصاص الجنائي العالمي[2].

2_ أن تكون الجريمة مرتكبة خارج إقليم تلك الدولة:

من أجل تطبيق مبدأ الإختصاص الجنائي العالمي، يجب أن تُرتكب الجريمة خارج إقليم الدولة التي تم فيها القبض على الجاني، لأنها إذا ارتكبت في إقليم هذه الدولة التي قُبِضَ فيها عليه فسيطبق مبدأ الإختصاص الإقليمي، ولا داعي لإخضاع هذه الجريمة لمبدأ الإختصاص الجنائي العالمي[3].

[1] وليد عبد الله سالم ال علي، مدى إنعقاد الإختصاص للقضاء الإماراتي بنظر أشد الجرائم الدولية الخطيرة وفقا لمبدأ الإختصاص الجنائي العالمي، مجلة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد 19، العدد1، مارس 2022، ص 296– 297.

[2] وليد عبد الله سالم ال علي، المرجع نفسه، ص298.

[3] وليد عبد الله سالم ال علي، المرجع نفسه، ص 302.

3_ إقامة مرتكب الجريمة على إقليم الدولة أو القبض عليه في إقليمها:

حتى يتم تطبيقه لابد من القبض على المتهم في إقليم دولة معينة، أو أن يتم القبض عليه في مكان ليس خاضع لسيادة دولة أخرى كالبحر العام مثلا[1].

4_ إزدواجية التجريم:

وهذا يعني أن الجرائم التي يحاكم المتهم بإرتكابها يجب أن ينص عليها القانون الوطني للدولة التي تم إرتكاب الأفعال الإجرامية فيها والدولة التي يوجد بها المتهم والتي ترغب في تطبيق مبدأ الإختصاص الجنائي العالمي في الدولة وقت إرتكاب هذه الأفعال المجرمة[2].

5_ عدم تسليم المتهم:

فيكون من غير الممكن تسليم المجرم إلى الدولة التي ارتكب فيها الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال الاستناد إلى مبدأ الإقليمية ومبدأ الشخصية[3].

الفرع الثاني: التوجه نحو تطبيق مبدأ الإختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن مبدأ الإختصاص الجنائي العالمي، أصبح يعتبر آلية من آليات التعاون الدولي في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ومكافحة إفلات المجرمين المعلوماتيين من العقاب، لذا اتجهت بعض الدول إلى الأخذ به وتطبيقه في الجرائم العابرة للحدود، وذلك لوجود عدة مبررات، لكن يعترض تطبيق عالمية النص الجنائي على هذه

[1] شوقي يعيش تمام، عزيزة شبري، تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي، مخبر أثر الإجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد 15، سبتمبر 2017، ص93.

[2] أحمد لطفي السيد مرعي، الولاية الجنائية العالمية (دراسة مقارنة)، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، مصر، (الجزء الأول)، المجلد 11، العدد 76، يونيو 2021، ص1131.

[3] بكري يوسف بكري محمد، قانون العقوبات القسم العام النظرية العامة للجريمة، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2013، ص217.

الجرائم عدة تحديات، من خلال هذا الفرع سنتطرق إلى مبررات تطبيقه في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (أولا)، الصعوبات التي تواجه تطبيق مبدأ الإختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (ثانيا).

أولا: مبررات تطبيق مبدأ الإختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن فكرة حماية المصالح العامة والمشتركة للبشرية قاطبة[1]، تعتبر المبرر الأساسي للأخذ بهذا المبدأ سواء في التشريعات الجنائية بصفة عامة أوفي نوع محدد من الجرائم والتي تمتاز بخطورة كبيرة، وتمتد أثارها لدول أخرى كالجرائم المنظمة، والجرائم الارهابية وجرائم الاتجار بالمخدرات، والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي هي موضوع دراستنا.

وإضافة إلى هذا المبرر الأساسي، فإن تطبيق هذا المبدأ في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يستند إلى مجموعة مبررات أخرى والتي تتمثل فيما يلي:

1_ خطورة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

حيث تعتبر هذه الجريمة من الجرائم العالمية الخطيرة المعاصرة، التي شهدت تزايد كبير بفضل تكنولوجيا المعلومات والاتصال، والقدرة على التنكر والاخْتِفَاء كاستخدام الأنترنت المظلم مثلا عند ارتكاب هذه الجرائم، هذا ما أدى إلى ظهور مجموعات إجرامية دولية منظمة تضم عددًا كبيرًا من المجرمين الذين ينتمون إلى جنسيات مختلفة ومتعددة، ويتسع نشاطهم ليمتد لأكثر من دولة[2].

[1] عبد الله أوهايبية، شرح قانون العقوبات الجزائري القسم العام، المرجع السابق، ص 158.

[2] بكري يوسف بكري محمد، المرجع السابق، ص214.

2_ ملائمة المبدأ للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

الإشكال الذي يثور لنا هو مدى ملائمة هذا المبدأ للتطبيق على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات؟ أهمية هذا المبدأ ومدى ملائمته للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، منبثقة من خطورة هذه الجريمة من جهة، ومن طبيعتها من جهة أخرى، كونها سهلة الوقوع من أشخاص يحملون جنسيات متعددة ومختلفة، والعناصر المادية لهذه الجريمة وسلوكياتها الإجرامية تمتد إلى أكثر من دولة، وفي وقت قصير جدا[1]، فهذه الجرائم عابرة للحدود الوطنية لأنها في غالب الأحيان يتم إرتكابها في حدود دولة معينة، ويكون ضحاياها في دولة واحدة أو أكثر، لأن هذه الأفعال تتم في فضاء معلوماتي لا حدود له، الأمر الذي يشكل صعوبة كبيرة لكل دول العالم دون استثناء[2].

فالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في أغلب الأحيان يتم إرتكابها عن بعد من قبل الجناة المعلوماتيين وبأساليب متطورة تتطور بتطور تكنولوجيات الإعلام والإتصال، مما يستوجب إخضاعها لمبدأ عالمية الإختصاص الجنائي، لأن خطورتها تفوق بكثير خطورة الجرائم العادية، باعتبارها يمكن أن تمتد إلى جميع دول العالم في لحظة واحدة، ونفس الشيء بالنسبة لمرتكبيها الذين يمتازون بالذكاء والخطورة التي تجعلهم يختلفون عن المجرمين التقليديين[3]، كونهم يكتسبون مختلف المهارات الفنية والتقنية ومُلِمّين بمختلف الأساليب المستحدثة التي ترتكب من خلالها الجريمة المعلوماتية بصفة عامة والجرائم المتعلقة بأنظمة معالجة المعطيات بصفة خاصة[4]، كما أن هذه الجرائم تفرض لمكافحتها إستخدام تقنيات خاصة لمكافحتها. فنظرا لخصوصيتها والخصائص التي تميزها من حيث

[1] خالد حسن أحمد لطيفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 111.

[2] شوقي يعيش تمام، عزيزة شبري، المرجع السابق، ص 94-95.

[3] قطاوي أمال، المرجع السابق، ص 94- 95.

[4] زراري نسرين، بوقرة إسماعيل، الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، المجلد 09، العدد 01، 2022، ص 109.

كونها عابرة لحدود الدول، فإنها أضفت أهمية بالغة على مبدأ الإختصاص القضائي العالمي في مجال مكافحة الجرائم المعلوماتية[1].

ومبدأ عالمية النص الجنائي يبقى عاجزا عن مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات إذا ما وجِد تعاون وتنسيق دولي جاد وسريع، وكذلك وجوب النص عليه بموجب النصوص الداخلية من خلال إمكانية معاقبة كل من يتم القبض عليه داخل إقليم الدولة دون مراعاة جنسية مرتكبها أو مكان وقوع الفعل الإجرامي، لكن ما يوجد فعليا أن أغلب الدول لم تنص على هذا المبدأ في تشريعاتها بالرغم من أن أغلب الاتفاقيات الدولية أكدت على تطبيقه كاتفاقية بودابست لمكافحة الجريمة المعلوماتية 2001، وكذلك القانون العربي النموذجي لمكافحة جرائم تقنية أنظمة المعلوماتية لسنة 2003 في المادة 26 منه[2].

وأهم ما يُجسد لنا هذه الملائمة ما يلي:

أ_ الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات عابرة للدول:

يفيد تعبير "جرائم عابرة للدول" أو جرائم عبر وطنية تلك الجرائم التي تقع بين أكثر من دولة، حيث أنها لا تعترف بالحدود الوطنية للدول[3]، مثلها مثل جُل الجرائم المنظمة، فلا معنى للحدود الجغرافية في هذه الجرائم، فهي لا تحترم الحدود السياسية، وترتكب حتى عن بعد، فالعالم بأسره يعتبر مسرحا لمرتكبيها، لأنه يمكن أن يكون الجاني في قارة والمجني عليه في قارة أخرى، فهذه الخصيصة هي التي تطبع على هذه الجرائم الصبغة العالمية[4].

[1] قطاوي أمال، المرجع السابق، ص 95.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 111- 112.

[3] أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية المعلومات الإلكترونية دراسة مقارنة، ط 3، دار الثقافة للنشر والتوزيع، عمان، 2017، ص 95.

[4] عبد الاله النوايسية، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمان، 2017، ص 78- 79.

إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا لا يعترف بالحدود الإقليمية للدول، ولا بالمكان، ولا بالزمان، أصبحت ساحتها العالم أجمع[1].

لأن مجتمع التقنية المعلوماتية " الإلكترونية" لا يعترف كما قلنا سابقا بالحدود الجغرافية ولا يتقيد بها لإنفتاحه عبر الزمان والمكان دون خضوعه للجانب التقليدي في الحراسة الدولية "حرس الحدود" فهذه التقنية تسمح لمستخدميها بالتنقل الافتراضي أو كما يطلق عليه التنقل المعنوي بين الدول والقارات دون أي تعقيد أو صعوبات أو عوائق، إنطلاقا من سهولة حركة المعلومات وتبادلها، هذا الذي جعل إرتكابها سهلا، حيث يتم إرتكاب السلوك الإجرامي في دولة وتتحقق النتيجة في دولة أخرى، وحتى إن أمكننا القول أنها تشترك في خاصية عبورها للحدود مع الجرائم التقليدية إلا أنها تختلف عنها في كون الجاني المعلوماتي لا يغادر مكانه ومقعده من أمام شاشة الحاسوب على خلاف تلك الجرائم التي تتطلب التحرك والنشاط الحركي[2].

فبفضل إنتشار شبكة الاتصالات العالمية للانترنت تم ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، مما سهل أمر الاتصال والترابط فيما بينها، فنظرا لطبيعة البيئة التي تُرتكب فيها هذه الجرائم وصفت الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بالجرائم العابرة للدول، لأنه غالبا ما يكون الجاني في بلد والمجني عليه في بلد أخر، كما قد يكون الضرر المتحصل في بلد ثالث في نفس الوقت، وعليه تعتبر هذه الجرائم شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الاقليمية أو القارية[3]، وما يجدر بنا الإشارة

[1] ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، 1438-2017، مقال منشور على الرابط التالي: https://www.ahewar.org/debat/show.art.asp?aid=571423
تم الإطلاع بتاريخ 2022/10/01 على الساعة09:09.

[2] عمار عباس الحسيني، المرجع السابق، ص 49.

[3] أسامة أحمد المناعسة، المرجع السابق، ص 95.

إليه أن هذه الخاصية أي أنها جريمة عابرة للحدود الوطنية أو الإقليمية أو القارية، قد خلقت الكثير من الإشكالات القانونية في مسألة الإختصاص القضائي والتحديات التي تقترن به[1].

ب_ فشل مبدأ إقليمية النص الجنائي في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

حيث أجمعت غالبية الاتفاقيات الدولية التي تكافح الجرائم المعلوماتية بصفة عامة عن عجز مبدأ إقليمية النص الجنائي في إستعاب الصور المتنوعة والمختلفة للنشاط الإجرامي في هذه الجرائم[2]، وذلك لارتطام هذا المبدأ بعقبة مادية تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي لأنه وكما هو معلوم أن مبدأ الاقليمية يقوم على أساس مكان وقوع الجريمة أو أحد عناصرها المادية، لأنه شرط أول لإنعقاد الاختصاص للقاضي الوطني، والذي من خلاله يترتب معرفة ما إذا كان الفعل مباحا في ذلك البلد أم مجرما، فهذا المبدأ يتضح أنه غير ملائم للجريمة المعلوماتية وذلك بالنظر لطبيعتها غير المادية من جهة ومن جهة أخرى لصعوبة اكتشافها وتحديد مكان وزمان وقوعها بدقة[3].

ج_ طبيعة الجريمة المعلوماتية الخاصة بسبب البيئة المرتكبة فيها الجريمة:

حيث ترتكب في بيئة تكنولوجيا المعلومات وهو الأمر الذي يجعلها تختلف عن الجرائم التقليدية، فأداة إرتكابها هو الحاسب الآلي وشبكة الانترنت، أما محلها فهو أنظمة معالجة المعطيات وبالضبط المعلومات المخزنة على الحاسوب وشبكاته[4] فهذه البيئة أكثر تعقيدا من البيئة التي ترتكب فيها الجرائم التقليدية[5].

---

[1] يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط 1، مطبعة الرمال، (الوادي)، الجزائر، جانفي 2019، ص29.

[2] قطاوي أمال، المرجع السابق، ص 95.

[3] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص107.

[4] أحمد عبد اللاه المراغي، المرجع السابق، ص 71.

[5] زراري نسرين، بوقرة إسماعيل، الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، المرجع السابق، ص 106.

3_ مساهمة مبدأ العالمية في التصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

من إخلال إرساء مبدأ العالمية يتم التصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث يعتبر هذا مبدأ عند تطبيقه على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات آلية للقضاء على الإفلات من العقاب للمجرمين المعلوماتيين.

فلهذا المبدأ أهمية كبيرة في ظل إنتشار الجرائم المعلوماتية بمختلف صورها، بما في ذلك الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، فنظرا لخصوصية هذا النوع من الجرائم وخطورتها الاجرامية، هذا ما جعلها تفرض نوعا من التعاون الدولي لمكافحة هذه الجريمة، خاصة في ظل الإشكالات القانونية التي تطرحها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لاسيما مشكلة تنازع الإختصاص[1].

ثانيا: الصعوبات التي تواجه تطبيق مبدأ الإختصاص الجنائي العالمي في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

1_ الصعوبات التي تواجه تطبيق مبدأ عالمية النص في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي ترجع إلى تطبيق المبدأ في حد ذاته:

أ_ مبدأ العالمية مبدأ منتقد:

يعتبر هذا الاختصاص في حد ذاته منتقدا من قبل الكثير من الدول، وحتى تلك الدول التي تعمل به وكانت تنادي به مثل بلجيكا التي أخذت تتراجع عنه، إلا أنه وفي الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والجرائم المعلوماتية بصفة عامة بعد إعتداءات 11 ديسمبر 2000 أصبحت تعتبر الجرائم المعلوماتية العابرة للحدود الوطنية كالجريمة المنظمة، الإرهاب الالكتروني، الجوسسة...الخ ذات طابع دولي كونها ترتكب في أكثر من دولة، ففرضت المصالح المشتركة للدول إعتماد هذا الإختصاص خاصة عندما تكون

[1] جمال زين العابدين أمين أحمد، المرجع السابق، ص86.

الأضرار خطيرة جدا، لكن في حدود إحترام حريات الأفراد وسيادة الدولة، على ضوء قواعد وأحكام تضبط هذا النوع من الاختصاص في بعض الجرائم المعلوماتية الخطيرة جدا[1].

ب_ التعارض مع فكرة السيادة الإقليمية:

إن تطبيق مبدأ العالمية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وإن كان يساهم في مكافحة هذه الجريمة في صورتها المستحدثة والمتطورة بشكل مستمر بسبب إستفادة المجرمين من التطور العلمي والتكنولوجي وإستغلاله في تنفيذ المشاريع الإجرامية، فإنه يتعارض يتعارض مع فكرة السيادة الإقليمية[2].

ج_ اصطدام هذا المبدأ مع مبدأ الشرعية:

يتعارض هذا المبدأ مع مبدأ من المبادئ الأساسية في القانون الجنائي وهو مبدأ الشرعية – شرعية الجرائم والعقوبات– الذي يتطلب تطبيق القانون الوطني على الجرائم التي تم النص عليها في قانون الدولة خاصة إذا كان القانون أصلح للمتهم، إضافة إلى أن تطبيقه يضع عقبات أمام القاضي الوطني تتمثل في ضرورة معرفته التامة وإلمامه بالقوانين الجنائية الموضوعية والإجرائية لمختلف الدول وهذا أمر أصعب، كما أن محاكمة المتهم الذي يتم تطبيق عليه هذا المبدأ يحمل الدولة أعباء مالية إضافية[3].

د_ صعوبة الفصل في الدعاوى:

فالدولة تلقى عناء في الفصل في الدعاوى التي تنشأ عن الجرائم التي تقع في إقليمها، لذلك فليس في طاقتها أن تضيف إلى ذلك مجهود آخر[4].

[1] مناصرة يوسف، المرجع السابق، ص 99– 100.

[2] عبد الله أوهايبية، شرح قانون العقوبات الجزائري القسم العام، المرجع السابق، ص 158.

[3] بكري يوسف بكري محمد، المرجع السابق، ص 215.

[4] أحسن بوسقيعة، الوجيز في شرح القانون الجزائي العام، المرجع السابق، ص 111–112.

هـ_ يطرح مبدأ عالمية النص الجنائي تنازع حاد بين التشريعات الجنائية في الدول:

يثير تطبيق هذا المبدأ تنازع في الاختصاص بين القوانين الجنائية للدول الأجنبية التي ارتكبت عليها والدول التي ينتسب إليها المجرم[1].

2_ الصعوبات التي تواجه تطبيق مبدأ عالمية النص في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي ترجع إلى خصوصية الجريمة:

أ_ غموض المفاهيم القانونية وإختلافها في الجرائم المعلوماتية:

ويرجع سبب هذا الغموض إلى عدم الاتفاق على مفهوم موحد للجريمة المعلوماتية، فالأنظمة القانونية للدول لم تضع صيغة محددة لهذه الجرائم[2]، وإن التشريعات الداخلية في الغالب لا تتضمن مفاهيم وتعريفات موحدة وأركان موحدة للجرائم المعلوماتية فكل تشريع يأخذ بمفاهيم تختلف عن تلك الموجودة في التشريعات الأخرى، وحتى في الاتفاقيات الدولية نفسها أحيانا لا نجد نفس التعريفات للجرائم المعلوماتية التي تتضمنها، وحتى وإن وجدت إتفاقية مثلا تكافح هذا النوع من الإجرام وصادقت عليها عدة دول فإن هذه الدول عند إدراج القواعد القانونية التي جاءت بها هذه الاتفاقية في تشريعاتها الداخلية غالبا ما لا تتطابق حرفيا مع ما وجد في تلك الاتفاقية.

ب_ إختلاف وتنوع النظم الإجرائية للدول:

يعتبر إختلاف وتنوع القواعد الإجرائية من الصعوبات التي تعترض تطبيق مبدأ العالمية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث بسبب هذا التنوع يمكن أن يعيق قانون الإجراءات الجزائية لدولة أخرى مباشرة بعض إجراءات التحري والتحقيق في هذه الجرائم، وكذلك يصعب إجراءات الملاحقة خارج إقليم الدولة، نظرا لاختلاف هذه

[1] بكري يوسف بكري محمد، المرجع نفسه، ص 215.

[2] لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، ط 1، دار الحامد، الأردن، عمان، 2015، ص254.

الإجراءات من دولة لأخرى، وبالتالي يفلت المجرمين من العقاب بسبب هذه الصعوبات، لكن يمكن إيجاد حل لهذه الصعوبات من خلال تشريع قانون إتفاقي موحد يعالج هذه المسألة[1].

وكذلك الإجراءات الجنائية المتعلقة بالبحث والتحري والتحقيق في هذا النوع من الجرائم قد تثبت نجاعتها في دولة ما يمكن أن تكون فاشلة ودون فائدة في دولة أخرى، ويمكن أن لا يسمح للجهات المختصة بالتحقيق بإجرائها أصلا[2].

ج_ نقص التنسيق والتعاون بين الدول:

فعلى الرغم من خطورة الجرائم المعلوماتية، إلا أن التنسيق والتعاون الدولي في هذا الصدد، لم يصل إلى مستوى الاهتمام الذي وصلت إليه بعض الجرائم العالمية كالإرهاب، وذلك لافتقار الدول إلى سبل تعاون دولي فيما بينها ، مما يوفر للمجرمين المعلوماتيين ملاذا آمنا لارتكاب جرائمهم هذه حول العالم دون معاقبتهم عليها، لذلك يجب توسيع نطاق التنسيق والتعاون الدوليين بشأن الجرائم المعلوماتية، وتعزيزه من خلال فتح قنوات الاتصال بين الدول، مما يتيح إمكانية إكتشاف الجرائم المعلوماتية وتبسيط وتسهيل إجراءات التحقيق وجمع الأدلة بشأنها[3].

د_ إشكالية تنازع القوانين وتنازع الاختصاص القضائي في الجرائم المعلوماتية:

يمكن حدوث تنازع إيجابي في الاختصاص في أكثر من تشريع وطني، وفي حالة إثارة التنازع تكون في الجرائم عبر الوطنية كالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي يتوزع السلوك المادي لها في أكثر من دولة[4].

[1] الطيب بلواضح، المرجع السابق، ص 194.

[2] لينا محمد الأسدي، المرجع السابق، ص 254.

[3] الطيب بلواضح، المرجع نفسه، ص 196.

[4] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 113.

وفي ختام هذا المطلب لابد علينا من التعرض لموقف المشرع الجزائري من مبدأ العالمية:

إن قانون العقوبات الجزائري، لم يُقر بالأخذ بمبدأ عالمية النص الجنائي على غرار غالبية التشريعات المقارنة لأنه أخذت به تشريعات قليلة، فحسب المشرع الجزائري فإن الجزائري الذي يرتكب جريمة من الجرائم التي تدخل في نطاق هذا المبدأ لا يفلت من العقاب، لأنه محكوم بالأحكام المقرة في المواد من 582- 584 من قانون الإجراءات الجزائية الجزائري المقررة لشخصية النص الجنائي[1].

وكذلك بالرجوع إلى قانون الإجراءات الجزائية الجزائري، نلاحظ أنه لم يكرس الإختصاص العالمي.

فغالبية الدول التي لم تأخذ به واستغنت عنه عوضته في مجال التعاون الدولي والتكاثف لمحاربة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بمبدأ شخصية النص الجنائي ومبدأ العينة وقواعد تسليم المجرمين[2].

إلا أنه من الناحية العملية نجد أن وزارة العدل تسعى جاهدة إلى عقد عدة إتفاقيات ونشاطات سواء على المستوى العربي أو الدولي لأجل مكافحة الإجرام المنظم بصفة عامة والجرائم المعلوماتية بصفة خاصة، غير أن هذه الإتفاقيات إن لم تُدعم بمبدأ عالمية النص الجنائي تبقى عاجزة عن مواجهة هذه الجرائم إن لم تكن الجريمة المرتكبة تخضع لسلطان القانون الجزائي الجزائري بمقتضى مبدأ الإقليمية أو الشخصية أو العينية، وبالرغم من تبني المشرع الجزائري لنظام التطبيق المباشر للمعاهدات الدولية بمجرد التصديق وفق المادة

[1] عبد الله أوهايبية، شرح قانون العقوبات الجزائري القسم العام، المرجع السابق ص157.

[2] عبد الله أوهايبية، شرح قانون العقوبات الجزائري القسم العام، المرجع نفسه، ص 159.

132 من دستور سنة 1996 المعدل والمتمم[1]، ونص المادة 171 من التعديل الدستوري لسنة 2020 بأنه "يلتزم القاضي في ممارسة وظيفته بتطبيق المعاهدات المصادق عليها، وقوانين الجمهورية وكذا قرارات المحكمة الدستورية" فمن خلال قراءة هذه المادة يتضح أن القاضي الجزائري ملزم بتطبيق المعاهدات والاتفاقيات الدولية المصادق عليها من طرف الدولة الجزائرية، مباشرة دون حاجة إلى إفراغها في قوانين داخلية، أو موائمة التشريعات الوطنية معها، والمشرع الدستوري في هذه المادة نص على القاضي بصفة عامة ولم يحدد ما إذا كان قاضي مدني، أم جزائي وبالتالي فهذه القاعدة تنطبق كذلك على القاضي الجزائي، لكن عند الرجوع إلى الاتفاقيات التي تكافح الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات نجد غالبيتها تحث وتلزم أحيانا الدول الاطراف على تجريم الأفعال التي تمس بأنظمة المعالجة الآلية للمعطيات، دون تحديد الجزاءات الجنائية، وبالتالي يصعب تطبيقها مباشرة.

وعند الرجوع إلى نص المادة 139 وبالضبط في المطة 7 منها حيث تنص هذه المادة أنه "يشرع البرلمان في الميادين التي يخصصها له الدستور، وكذلك في المجالات الآتية:

..... 7)- القواعد العامة لقانون العقوبات، والإجراءات الجزائية، لاسيما تحديد الجنايات والجنح، والعقوبات المختلفة المطابقة لها، والعفو الشامل، وتسليم المجرمين، ونظام السجون" يستشف أن القاضي لا يمكنه مباشرة تطبيق الاتفاقيات الدولية في مجال التجريم والعقاب، فالمادة الجنائية يستحيل فيها التطبيق المباشر للاتفاقية، وإنما يجب النص على الجريمة أو الإجراء الجزائي بموجب قانون مستحدث، أو موائمة التشريعات الموجودة مع ما هو وارد في الاتفاقية الدولية المصادق عليه، ونشرها في الجريدة الرسمية، حتى تعتبر نافذة.

[1] عبد المومن بن صغير، تطبيق النص الجنائي بين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية بجامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 10، العدد03، ديسمبر 2019، ص78.

وما يجدر بنا الإشارة إليه في ختام هذا المطلب هو أن الفقه أصبح يندد بإلزامية ظهور فرع جديد من فروع القانون الجنائي الدولي وهو القانون الجنائي الدولي للمعلوماتية والأنترنت. وحتى نشهد ولادته القريبة لابد من بذل المزيد من الجهد الفقهي والتشريعي[1].

المبحث الثاني: التعاون الجنائي الدولي في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن تأمين الأدلة الرقمية عبر الحدود والبحث والتحري والتحقيق في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، في كثير من الأحيان يفتقر إلى الأطر القانونية، وخاصة الإجرائية منها بهدف الحفاظ على الأدلة الرقمية والتحقيق في الجرائم الإلكترونية، وهذا يشكل عقبة رئيسية نظرًا لأن معظم هذه الهجمات يتم تنظيمها عادةً من طرف الجماعات الإجرامية المنظمة المتواجدة في ولايات قضائية مختلفة، هذا ما أبرز الحاجة الواضحة للتعاون القضائي الجنائي الدولي، ولا سيما التعاون الوثيق على المستوى العالمي خاصة في ظل وجود البيانات الرقمية التي يمكن تداولها عبر الدول لأجل تنظيم حركة مرورها بين هذه البلدان، وكذلك لتسهيل إجراءات التحقيقات وإجراءات إنفاذ القانون مع الدول الأخرى من خلال نشر فرق تحقيق مشتركة من أجل التمكن من تتبع وتحديد مكان المشتبه بهم.

والتحقيقات في الجرائم الإلكترونية عبر الحدود معقدة وطويلة وغالبا لا تصل إلى النتيجة المرجوة[2].

لذا يعتبر التعاون القضائي من أهم آليات التعاون الدولي كونه يتمثل في مجموع الوسائل القانونية التي بواسطتها يتم تقديم المعاونة من طرف إحدى الدول إلى دولة أخرى

[1] العنكبي نزار، المرجع السابق، ص90.

[2] Cristos Velasco, Cybercrime and Artificial Intelligence.An overview of the work of international organizations on criminal justice and the international applicable instruments, Journal of the Academy of European La,Volume 23, issue 1, May 2022, p114 .

بشأن التحقيق أو المحاكمة أو التنفيذ[1]، ويتمثل التعاون القضائي الجنائي الدولي في التعاون الشرطي الدولي (المطلب الأول)، والمساعدة القضائية وتسليم المجرمين (المطلب الثاني).

المطلب الأول: التعاون الشرطي الدولي في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

لدعم وتعزيز التعاون الدولي في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي تتميز بخصوصية عبورها للحدود الوطنية، الذي تعترضه السيادة الوطنية وتعرقل مواجهتها، لذا تم الاعتماد على التعاون الشرطي الدولي أو كما يطلق عليه التعاون الأمني حتى يتم القبض على الجناة مختلفي الجنسيات، وتبادل المعلومات بين الأجهزة الشرطية حول المجرمين والجرائم في مختلف دول العالم، ودعم الإجراءات من خلال التعاون التقني بينها، والبحث والتحري على هذه الجرائم، هذا ما أدى إلى بروز التعاون الشرطي على المستوى العالمي من خلال المنظمة الدولية للشرطة الجنائية (الفرع الأول)، وكذلك ظهور التعاون الشرطي على المستوى الإقليمي (الفرع الثاني).

الفرع الأول: المنظمة الدولية للشرطة الجنائية

إن جهود الانتربول في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ومكافحتها، من خلال ضباط الارتباط المنتشرين في كافة دول العالم والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق لمكافحة والتصدي لهذه الجرائم[2].

بدأ هذا النوع من التعاون على صورة مؤتمرات أولها مؤتمر موناكو سنة 1914 والذي ضم كل من رجال الشرطة والقضاء والقانون، وتبادل المؤتمر بالمناقشة لبعض المسائل التي تتعلق بالشرطة، وفي سنة 1923 تم عقد مؤتمر دولي ثاني على المستوى الدولي للشرطة الجنائية، وكانت أهم نتيجة له هي إنشاء لجنة دولية للشرطة الجنائية في فيينا مهمتها

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 77.

[2] أسامة أحمد المناعسة، جلال محمد الزعبي، المرجع السابق، ص 96.

التنسيق بين أجهزة الشرطة، ثم توقف عمل هذه اللجنة، ثم تم عقد مؤتمر في بروكسل 1946 تم إحياء هذه اللجنة ونقل مقرها إلى باريس و أكدت هذه المنظمة على ضرورة تفعيل التعاون بين الدول الأطراف في مجال مكافحة الجريمة المعلوماتية[1].

وتم تغيير اسمها إلى المنظمة الدولية للشرطة الجنائية، هدفها هو تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة، عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمة إليها، وتتبادلها فيما بينها بالإضافة إلى التعاون في ضبط المجرمين بمساعدة الشرطة في الدول الأطراف، ومدها بالمعلومات المتوفرة لديها على إقليمها وخاصة بالنسبة للجريمة المعلوماتية كونها متشعبة في عدة دول.

ومرت جهود المنظمة في هذا المجال بمراحل عديدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية في طوكيو، نيوزيلندا، نيروبي، أذربيجان، بيونس أيرس، ومكتب إقليمي فرعي في بانكو[2]، وعلى هذا الأساس تم إنشاء الشرطة الأوربية سنة 1991 من قبل المجلس الأوربي هدفها ملاحقة الجناة في الجرائم العابرة للحدود ومنها جرائم الكومبيوتر[3].

وما يجدر الإشارة إليه أن جميع الدول الأعضاء في هذه المنظمة لديهم مكتباً مركزي وطني للانتربول[4] (NCB) ويوفر هذا المكتب الاتصال بين أجهزة إنفاذ القانون في هذه

[1] لينا محمد الأسدي، المرجع السابق، ص101.

[2] محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة– بجاية، الجزائر، المجلد 14، العدد02، 2016، ص54.

[3] لينا محمد الأسدي، المرجع نفسه، ص101.

[4] المكاتب المركزية الوطنية (NCBs) مهامها الحصول على المعلومات الضرورية من المكاتب المركزية الوطنية الأخرى لمساعدتها على التحقيق في الجريمة أو مع المجرمين في بلدها، وتتقاسم البيانات الجنائية والمعلومات الاستخباراتية لمساعدة دولل آخر.

الدولة، مع الدول الأخرى الأعضاء والأمانة العامة من خلال شبكة اتصالات الشرطة العالمية الآمنة عبر منظومة الاتصالات العالمية للشرطة[1].

وتعتبر الجزائر إحدى الدول الأعضاء في المنظمة الدولية للشرطة الجنائية أنتربول، منذ أن إنعقدت الجمعية العامة للأنتربول بهلسنكي/فنلندا، في أوت 1963، بمشاركة 53 دولة، ممثلة بالمكتب المركزي الوطني[2]، حيث يعمل المكتب المركزي الوطني تحت الإشراف المباشرة للمديرية العامة للأمن الوطني، ويمارس مهامه طبقا للنصوص التشريعية الوطنية، مع إلتزامه بقوانين منظمة الانتربول[3].

تساهم هذه المكاتب في إدراج بيانات الجريمة الوطنية مع قواعد بيانات الانتربول العالمية، وفقاً للقوانين الوطنية الخاصة بكل منها. وتتعاون في التحقيقات والعمليات والاعتقالات عبر الحدود. للتفصيل أكثر إطلع على الموقع الرسمي للانتربول، متوفر على الرابط التالي: https://www.interpol.int/ar/3/10/1/1.

تم الاطلاع عليه يوم 02/ 06/ 2022 على الساعة 21:25.

[1] أنظر الموقع الرسمي للانتربول، متوفر على الموقع التالي:

https://www.interpol.int/ar/3/10/1/1 تم الاطلاع عليه يوم 02/ 06/ 2022 على الساعة 22:00.

[2] يجب على المكتب المركزي الوطني أن ينفذ أنشاطته في إطار إستراتجية واضحة ومحددة بشكل جيد وفقا لما للاحتياجات الأمنية المسجلة على المستوى الوطني، في إطار المهام الأساسية التي حددتها المنظمة الدولية للشرطة الجنائية، خدمات اتصالات شرطية عالمية مأمونة، خدمات بيانات ميدانية وقواعد بيانات شرطية، للتفصيل أكثر إطلع على الموقع الرسمي للمديرية العامة للأمن الوطني، متوفر على الرابط التالي:

https://www.algeriepolice.dz/?-%D8%A7%D9%84%D8%AF%D9%88%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%A7%D8%A8%D9%82%D8%A9

تم الاطلاع عليه يوم 03/ 06/ 2022 على الساعة 9:06.

[3] الموقع الرسمي للمديرية العامة للأمن الوطني، متوفر على الرابط التالي:

https://www.algeriepolice.dz/?-%D8%A7%D9%84%D8%AF%D9%88%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%A7%D8%A8%D9%82%D8%A9

تم الإطلاع عليه بتاريخ: 2022/06/03 على الساعة 11:35.

أولا: دور المنظمة الدولية للشرطة الجنائية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

فتهدف المنظمة الجنائية للشرطة الدولية (الإنتربول) إلى تحقيق هدفين أساسيين يتمثل أولهما في ضمان وتنمية التعاون على نطاق واسع بين كافة سلطات الشرطة الجنائية وذلك في إطار القوانين السارية المفعول في مختلف البلدان ووفقا للإعلان العالمي لحقوق الإنسان، أما الهدف الثاني فيتمثل في إنشاء وتنمية كل المؤسسات القائمة على المساهمة الفعالة في الوقاية من جرائم القانون العام ومكافحتها[1].

تعتبر مهمة الانتربول مهمة أساسية في مجال مكافحة الجرائم المنظمة العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة ولاسيما تلك المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث هذه الهيئة تفعل التعاون من خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات بغرض تسهيل عملية التحقيق لضبط وملاحقة المجرمين المعلوماتيين، وكذلك هؤلاءك الهاربين وتقوم بتسليمهم إلى الدولة طالبة التسليم[2].

وتقوم بهذه المهام المكاتب المركزية والوطنية التي يتواجد مقرها في كل دولة عضو وإلى جهاز دائم يتم تعيينه بواسطة السلطات الحكومية الوطنية وبمساعدة فرق الانتربول التي يمكنها التحرك لموقع الحدث بغرض تسهيل التحقيق والتحليل في مكان الحدث وذلك بالتنسيق مع الامانة العامة، في تعميم نشر التحذيرات المتنوعة التي تحتوي على المعلومات الاستخباراتية والاحاطات والمشورة الفنية عن الاخطار الاجرامية المحتمل وقوعها[3].

---

[1] أنظر المادة 2 من القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الإنتربول)، للإطلاع على هذا القانون باللغة العربية، متوفر على الرابط التالي:

file:///C:/Users/user/Downloads/01%20A_Constitution%20(1).pdf

[2] شيخة حسين الزهراني، المرجع السابق، ص 745.

[3] شيخة حسين الزهراني، المرجع نفسه، ص 745.

فتقوم في مجال مكافحة الجرائم المعلوماتية بوضع قائمة تتضمن أسماء الضباط المختصين الذين يمكن الاستعانة بهم في عمليات البحث والتحري عن الجرائم المعلوماتية، وتوفر للدول الأطراف مختلف المعلومات اللازمة التي تبين الطرق العملية في مجال مكافحة هذه الجريمة من خلال تكوين فرق عمل لوضع الأسس العلمية والعملية للمكافحة[1].

وتستخدم هذه المنظمة عدة وسائل فنية في مكافحة الجريمة المعلوماتية من بين هذه الوسائل النشرات الدولية التي تصدرها الأمانة العامة بناء على طلب يقدم لها من المكاتب المركزية الوطنية للدول الأعضاء، وتتنوع هذه النشرات حسب مضمونها والهدف منها[2]، وكذلك البحث والتقصي في قواعد البيانات وتقديم الخبرات والدورات التدريبية في مجال مكافحة الجرائم المعلوماتية من خلال إستعانتها بمجموعة من الخبراء الدوليين والمختبرات الدولية على الصعيد العالمي، ناهيك عن تسهيل تبادل وتحليل المعلومات والبيانات الجنائية وتخزينها، وتقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول جرائم الانترنت وكيفية التدريب على مكافحتها والتحقيق فيها[3].

وقامت هذه المنظمة بإنشاء وحدة متخصصة لمكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الجرائم وكيفية التدريب على مكافحته[4].

وللمنظمة الدولية للشرطة الجنائية في مجال النشاط الشرطي دور لايستهان به حيث تقوم بإجراءات التحقيق الدولية بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من وإلى خارج الوطن وذلك من خلال التنسيق مع المصالح الوطنية ونظيرتها في الدول

[1] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 92.

[2] جيلالي الحسين، التعاون الجنائي الدولي في مكافحة الجريمة العالمية، مجلة القانون، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد زبانة بغليزان، الجزائر، المجلد07، العدد02، 2018، ص22.

[3] شيخة حسين الزهراني، المرجع السابق، ص 745.

[4] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع نفسه، ص92.

الأجنبية، وتقدم الدعم الفني والتقني إلى جميع الأجهزة والمصالح الوطنية المكلفة بإنفاذ القانون، إضافة إلى التبادل الآني للمعلومات الشرطية والجنائية ما بين المكاتب المركزية الوطنية، وذلك يكون بالتنسيق مع الأمانة العامة لمنظمة الأنتربول، وتصدر مختلف نشرات البحث بغرض القيام بالتحريات والتحقيقات وتقوم بجمع المعلومات العملياتية، وتحليلها لأجل البحث والتحري عن هذه الجرائم، إضافة إلى ذلك تلاحق المجرمين الفارين والذين هم محل بحث دوليا، بغرض إيقافهم و تسليمهم[1].

ثانيا: آليات المنظمة الدولية للشرطة الجنائية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

من أبرز آليات المنظمة الدولية للشرطة الجنائية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أنها انتهجت استراتيجية خاصة لمكافحة هذا النوع المستحدث من الجرائم، إضافة إلى إنشائها المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرانية إضافة إلى مخبر الأدلة الرقمية، إنشاء مديرية الجرائم الالكترونية للانتربول.

1_ إستراتيجية الانتربول في مكافحة الجرائم المعلوماتية:

إن خصوصية الجرائم السيبرانية جعلتها من أسرع أشكال الجرائم العابرة للحدود الوطنية. وذلك لاعتمادها بشكل كبير على الأنترنت، مما خلق مخاطر المعلوماتية متعددة وجعلها تتفاقم، خاصة ببروز نقاط ضعف الأنظمة المعلوماتية، وبسبب الطبيعة الخاصة لهذه الجرائم والتحديات التي تواجه التحقيق العابر للحدود، إضافة إلى التحديات القانونية، هذا ما تطلب ضرورة وضع إستراتيجية شاملة واضحة الأهداف لمواجهة هذه الجرائم ومختلف تحدياتها.

[1] الموقع الرسمي للمديرية العامة للأمن الوطني، متوفر على الرابط التالي:
https://www.algeriepolice.dz/?-%D8%A7%D9%84%D8%AF%D9%88%D8%B1%D8%A7%D8%AA-%D8%A7%D9%84%D8%B3%D8%A7%D8%A8%D9%82%D8%A9
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة07:01.

وضعت المنظمة الدولية للشرطة الجنائية (الانتربول) برنامجين عالميين متعلقين بمكافحة جرائم الإرهاب والجريمة المنظمة، بهدف مكافحة مختلف أشكال الجريمة العابرة للحدود الوطنية، إضافة إلى ذلك وضعت الانتربول إستراتيجية لمكافحة الجرائم المعلوماتية موسومة ب " **الاستراتيجية الشاملة لمكافحة الجريمة السيبرية**"

فهذه الاستراتيجية توضح الخطة التي انتهجتها المنظمة الدولية للشرطة الجنائية (الانتربول) لمساندة الجهود التي تبذلها الدول الأعضاء في مجال مكافحة الجرائم السيبرية وذلك من خلال تنسيقه وتوفيره الامكانية الشرطية المتخصصة، وتقوم الانتربول بمراجعة هذه الاستراتيجية التي وضعتها بشكل دوري حتى تبقى مرتبطة بالواقع الراهن وتتماشى مع التهديدات الناشئة في البيئة الرقمية التي تتميز بالديناميكية وتستجيب لتطلعات البلدان الأعضاء[1].

والهدف الأساسي لبرنامج الإنتربول لمكافحة الجرائم السيبرية هو استهداف ‘‘الجرائم السيبرية المحض’’ أي جرائم المساس بأنظمة المعالجة الآلية للمعطيات[2].

[1] الموقع الرسمي للانتربول، متوفر على الربط التالي:
file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_AR_LR.pdf
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 11:37.

[2] الموقع الرسمي للانتربول، متوفر على الربط التالي:
file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_AR_LR.pdf
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 11:45.

وتضمنت هذه الاستراتيجية الشاملة لمكافحة الجرائم السيبرية خمس مسارات عمل كالتالي:

أ_ تقييم التهديدات وتحليلها ورصد اتجاهاتها:

ويكون ذلك من خلال الكشف عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ومرتكبيها والمجموعات التي تقف وراءها، وهذا يتم التوصل إليه بعد تقييم التهديدات السيبرانية وتحليلها ورصد اتجاهاتها، والوصول إلى نتائج مؤكدة.

ب_ الإطلاع على البيانات الرقمية الأصلية والإستفادة منها:

من خلال تيسير الوصول إلى مختلف البيانات والمعطيات المتعلقة بالإعتداءات السيبرية بأشكالها المتعددة، لتعزيز جمع البيانات والإستفادة منها بشكل أفضل[1]، والاستفادة من الإحصائيات المتعلقة بها.

ج_ إدارة الأدلة الرقمية:

إدارة الأدلة الرقمية لأغراض التحقيقات والملاحقات القضائية: من خلال جمع القرائن الرقمية وفقا للقانون، وحفظ الأدلة وعرضها بشكل مفهوم وواضح ومقبول لدى المحاكم.

د_ الربط بين المعلومات السيبرية والمعلومات الفعلية:

العثور على العلاقة القائمة بين الأدلة الرقمية والمعلومات الفعلية ليتسنى تحديد مكان المرتكبين المحتملين لهذه الجرائم.

[1] الموقع الرسمي للانتربول، متوفر على الربط التالي:
file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_AR_LR.pdf
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 11:54.

هـ_ التوحيد والتشغيل البيني:

من خلال التنسيق على المستوى العالمي والحث على توحيد التشريعات[1].

ويتم تنفيذ هذا البرنامج من قبل مجمع الانتربول العالمي للابتكار الموجود في سنغافورة الذي يضم مركز متعدد الاختصاصات لمكافحة الجرائم السيبيرية ومختبر للأدلة الرقمية ومركز ابتكار. سنفصل فيها لاحقا، ويتم دعم هذه البرامج من طرف المنظمة من خلال إدارة البيانات الشرطية، وتحليلها جنائيا، ودعم الأدلة الرقمية الجنائية، والتأهيل والتدريب، والابتكار[2].

2_ إنشاء المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية في الانتربول:

أنشأت المنظمة الدولية للشرطة الجنائية التي تضم 190 دولة عضو، المجمع العالمي للابتكار (IGGI)، في سنغافورة بدأ هذا المركز مهامه في سنة 2015، كمؤشر بداية بانتقال الشرطة العالمية إلى العصر الرقمي[3]، والذي فيه تم إنشاء مركز متخصص لمكافحة الجريمة السيبرانية.

وذلك تماشيا مع الأمن الرقمي الذي يعتبر حاليا من أهم ركائز المجمع العالمي، لهذا تم إنشاء هذا المركز الذي يضم خبراء من أجهزة إنفاذ القانون والشركات والأكاديميين بغرض رصد وجمع وتحليل البيانات الاستخباراتية المتعلقة بالتهديدات السيبرانية، والجرائم السيبرانية.

[1] الموقع الرسمي للانتربول، متوفر على الربط التالي:
file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_AR_LR.pdf
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 12:02.

[2] الموقع الرسمي للانتربول، متوفر على الربط التالي:
file:///C:/Users/user/Downloads/Summary_CYBER_Strategy_2017_01_AR_LR.pdf
تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 15:00.

[3] Vendius, Trine Thygesen , Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene, Published in: European Journal of Policing Studies , 2015, P153.

فهذا المركز العالمي، يمثل الجزء الحيوي للإنتربول الذي يقوم بالاستخبارات والتنسيق العملياتي بشأن التهديدات السيبرانية، ويسهل عمليات تبادل المعلومات بين أجهزة الشرطة ويقدم معلومات استخباراتية بخصوص التهديدات التي محلها الفضاء السيبراني[1]

وينشر المركز تقارير بغرض تنبيه الدول إلى التهديدات السيبرانية بكل أنواعها وخاصة المستحدثة منها. ومنذ سنة 2017 أصدرت هذه المنظمة أكثر من 800 تقرير موجه للشرطة في أكثر من 150 بلدا[2].

3_ إنشاء مخبر الأدلة الرقمية:

حيث يضم مجمّع إبتكار مخبر للأدلة الرقمية الجنائية، يساعد هذا الأخير على إيجاد حلول عملية من خلال تعاونه مع أجهزة الشرطة ومخابرت البحوث والجامعات وبإشراكه لكل من القطاع العام والخاص[3].

4_ إنشاء مديرية الجرائم الالكترونية للانتربول:

تقوم بعدة مهام حيث تقوم بدعم التحقيقات في الجرائم السيبرانية الرقمية، والتدريب على هذا النوع من الجرائم، وتنسق وتسهل إجراءات التحقيق العابرة للحدود الوطنية بخصوص هذا النوع من الجرائم، بما في ذلك تبادل المعلومات الاستخباراتية وتقديم المشورة بشأن أفضل الممارسات في إجراء التحقيقات في الجرائم الإلكترونية، وتقوم بتطوير الذكاء الإلكتروني لمكافحة الجرائم الإلكترونية ومعالجتها[4].

---

[1] الموقع الرسمي للانتربول، متوفر على الربط التالي:
https://www.interpol.int/ar/1/1/2014/35 تم الاطلاع عليه بتاريخ 2022/06/08 على الساعة 15:15.

[2] أنظر الموقع الرسمي للانتربول، متوفر على الربط التالي: https://www.interpol.int/ar/4/6/1
تم الإطلاع عليه بتاريخ 06/08/ 2022 على الساعة 11:40.

[3] أنظر الموقع الرسمي الموقع الرسمي للانتربول، متوفر على الربط التالي: https://www.interpol.int/ar/4/6/1
تم الإطلاع عليه بتاريخ 06/08/ 2022 على الساعة 11:40.

[4] الموقع الرسمي للانتربول، متوفر على الربط التالي:

الفرع الثاني: التعاون الشرطي (الأمني) على المستوى الاقليمي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

رغم وجود الشرطة الجنائية الدولية التي تعمل على مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، على المستوى العالمي، إلا أن هذه الجرائم استفحلت بشكل كبير بسبب أساليب إرتكابها المستحدثة، والمتطورة بشكل دائم لذا يتطلب تنسيق التعاون الشرطي على المستوى الإقليمي بين الدول بغرض الحد من هذه الجرائم بشكل متكامل مع التعاون الشرطي العالمي، حتى يتم تطويق هذه الجريمة ومحاصرتها عالميا، وإقليميا، وتضييق نطاقها كونها عابرة للحدود الوطنية ومنظمة ومستحدثة.

ومن خلال هذا الفرع سنتطرق إلى التعاون الشرطي على المستوى الأوروبي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (أولا)، التعاون الشرطي على المستوى الافريقي والعربي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (ثانيا).

أولا: التعاون الشرطي على المستوى الأوروبي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تم إنشاء على المستوى الأوربي أجهزة شرطة هدفها تنسيق التعاون بين الدول الأوربية لغرض مكافحة مختلف أنواع الإجرام التقليدي والمستحدث بما فيها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال تنسيق الجهود الأوربية في هذا الشأن وتتمثل في:

https://rm.coe.int/3148-3-2-eurojust-presentation-interpol-approach-ukim-v2/1680791601
تم الاطلاع عليه بتاريخ 05/ 06/ 2022 على الساعة 11:45.

1_ دور الشرطة الاوروبية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

ويطلق عليها تسمية **ديوان البوليس الأوربي**، أو **الأوروبول** والذي تأسس بموجب قرار مجلس الاتحاد الأوربي المؤرخ في 6 أفريل 2009 رقم JHA/ 2009/394 [1].

والهدف الأساسي لهذا الجهاز هو تيسير تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، ويقوم كذلك بتجميع المعلومات والبيانات وتحليلها لأجل المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص أي جريمة وبالأخص الجريمة المعلوماتية[2].

ويعتبر الأوروبول من أكبر الأجهزة الإستشارية في العالم بخصوص الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المعلوماتية، وذلك من خلال دعمه للحكومات والأجهزة الأمنية والمؤسسات لمجابهة أخطار هذه الجرائم، وتم إختياره من طرف الاتحاد الدولي للأمن المعلوماتي، لإنجاز مختلف الدراسات الخاصة بهذا النوع من الإجرام المستحدث إلى غاية سنة 2020 بهدف تحليل أسباب ودوافع إرتكاب الجرائم المعلوماتية، ووضع تصور مستقبلي للتطوراتها، وتم كذلك إختياره من قبل اللجنة الأوروبية كمركز إعلام حول موضوع الجرائم المعلوماتية[3]. وتم إنشاء جهاز على مستوى الاوروبول، بهدف التنسق أكثر بين الدول الأعضاء في مجال مكافحة الجريمة المعلوماتية يطلق عليه تسمية "ICROS"[4]، وتم إشاء جهاز EC3 لمكافحتها كذلك.

---

[1] كعرار سفيان، الآليات المؤسساتية الأوروبية لمكافحة الجريمة المنظمة عبر الوطن، المجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر، المجلد الرابع، العدد الأول، 2020، ص576.

[2] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 92- 93.

[3] حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة لنيل شهادة الدكتوراه ل.م.د في القانون العام تخصص قانون جنائي وعلم الإجرام، جامعة الجزائر 1، كلية الحقوق، الجزائر، 14 سبتمبر 2020، ص 271.

[4] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع نفسه، ص 93.

أ_ إنشاء المركز الأوربي للجرائم الإلكترونية على مستوى الاوروبول:

يعتبر إنشاء المركز الأوربي للجرائم الإلكترونية Centre européen de lutte contre la cybercriminalité (EC3) أول خطوة على المستوى الأوروبي لمواجهة التهديدات المتزايدة من الجرائم الالكترونية[1]، والذي يعتبر وحدة متخصصة لمكافحة الجرائم الالكترونية[2]، وتم ذلك في يناير 2013، إن إنشاء EC3 داخل اليوروبول أدى إلى استمرارً لبعض المهام التي كانت موجودة داخل اليوروبول، والتوسع في أخرى كانت موجودة من قبل، وخاصة الدعم التحليلي لتحقيقات الدول الأعضاء، إضافة إلى استحداث وظائف جديدة تتلائم مع طبيعة هذا المركز، حيث من مهام EC3 التركيز على المجالات الثلاثة التالية:

_الجرائم الالكترونية التي ترتكبها الجماعات المنظمة، ولا سيما تلك التي تحقق منها الجماعة الاجرامية المنظمة أرباح كبيرة مثل الاحتيال عبر الإنترنت.

_الجرائم الإلكترونية التي تسبب ضررًا جسيمًا لضحاياها، مثل الاستغلال الجنسي للأطفال عبر الانترنت.

_الجرائم الإلكترونية (بما في ذلك الهجمات الإلكترونية) التي تؤثر على البنية التحتية والمعلومات الحيوية في أنظمة في الاتحاد الأوروبي[3].

[1] Vendius, Trine Thygesen , Op.Cit, P153.

[2] Vittorio Guarriello, Emanuele Macrìe Silvio Marco Guarriello, Cybercrime : una nuova minaccia per la Pubblica Sicurezza , Democrazia e Sicurezza – Democracy and Security Review, anno XII, n. 1, 2022, p30.

[3] أنظر الموقع الرسمي للأوروبول، متوفر على الرابط التالي:

https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf

تم الاطلاع عليه بتاريخ 2022/06/10 على الساعة 10:27.

ب _ دور المركز الأوربي للجرائم الإلكترونية في مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

دوره الأساسي يتمثل في التعاون مع مختلف مراكز الشرطة في أوربا لمكافحة الأفعال غير المشروعة التي تنفذ على مستوى الفضاء السيبراني[1]، حيث يعزز مركز الجرائم الالكترونية القدرات على تحليل الجرائم الإلكترونية والتحقيقات، ويقوم بتعزيز التعاون مع الدول الأعضاء والشركاء الدوليين من القطاع الخاص، ويقيم ويراقب التدابير الوقائية من الجرائم الالكترونية وتقييم التحقيقات، إضافة إلى أنه يدعم تطوير مبادرات التدريب والتوعية بالقانون لأجهزة الشرطة والسلطة القضائية. ويسهل تقديم الشكاوي عن الجرائم الإلكترونية ويبسط المعالجة اللاحقة للمعلومات، من طرف أجهزة الشرطة في الدول الأعضاء والتنبيه من الجرائم الالكترونية من خلال المنصات الالكترونية، إضافة إلى تطوير التعاون مع الشبكة الأوروبية ووكالة أمن المعلومات(ENISA)، وكذلك فرق الاستجابة للطوارئ الحاسوبية الوطنية/الحكومية (CERTs) بشأن جوانب إنفاذ القانون ذات الصلة بالأمن السيبراني.

وما يجدر الاشارة إليه هنا أن رغبة الاتحاد الأوربي في بناء أمن سيبراني قوي للاتحاد الأوروبي جعلتها تؤكد على وجوب تطوير القدرة في الطب الشرعي السيبراني من طرف اليوروبول وتعزيز التحقيقات على شبكة الانترنت المظلمة، إضافة إلى إيلاء عناية بالتكنولوجيات التي تعتمد بشكل كبير على إساءة استخدام التشفير من طرف المجرمين المعلوماتيين كونها تشكل تحديات تواجه مكافحة الجريمة المنظمة الالكترونية والارهابية[2].

[1] Vittorio Guarriello, Emanuele Macrìe Silvio Marco Guarriello, Op.cit, p30.

[2] أنظر الموقع الرسمي للأوروبول، متوفر على الرابط التالي:
https://parleu2020.sabor.hr/sites/default/files/dogadaji/2020-03/Europol%20Programming%20Document%202020-2022.PDF
تم الاطلاع عليه بتاريخ 2022/06/10 على الساعة 05:30.

علاوة على ذلك، ظهر نوع جديد من الهجمات الإلكترونية التي تستند إلى أنظمة الذكاء الاصطناعي، وهي نوع جديد ظهر بشكل متزايد حدده المركز الأوروبي للجرائم الإلكترونية (EC3) التابع لليوروبول من خلال تقرير تقييم تهديدات جرائم الإنترنت لسنة 2020، وشدد EC3 على أن المخاطر المتعلقة باستخدام الذكاء الاصطناعي لأغراض إجرامية يجب فهمها جيدًا من أجل حماية المجتمع من الجهات الخبيثة، وفقًا لـ EC3 فإنه من خلال الذكاء الاصطناعي، يمكن للمجرمين تسهيل وتحسين هجماتهم من خلال تعظيم فرصهم في تحقيق الربح في فترة زمنية أقصر وإنشاء نماذج أعمال إجرامية أكثر ابتكارًا، مع تقليل إمكانية تعقبها والتعرف عليها من قبل السلطات المختصة، إضافة إلى ذلك يوصي EC3 بتطوير المزيد من المعرفة حول الاستخدام المحتمل للذكاء الاصطناعي من قبل المجرمين بغرض توقع أفضل الأنشطة الخبيثة والإجرامية المحتملة التي يُسهل ارتكابها الذكاء الاصطناعي، وكذلك للوقاية من هذه الهجمات استباقيا، أو لتخفيف آثارها، وذلك بالتعاون مع والأوساط الأكاديمية[1].

فيما يتعلق بالمجالات الثلاثة السابقة الذكر، فإن مهام EC3 تتمثل في أنه يعمل بمثابة محور مركزي للمعلومات والاستخبارات الجنائية، إضاف إلى أنه كما سبق وذكرنا يدعم التحقيقات في الدول الأعضاء وذلك من خلال التحليل العملي والتنسيق بينها والخبرة، ويوفر مجموعة متنوعة من منتجات التحليل الاستراتيجي التي تمكن من اتخاذ قرارات مستنيرة في مجال مكافحة ومنع الجرائم السيبرانية، وإنشاء وظيفة توعية شاملة تربط أجهزة إنفاذ القانون ذات الصلة بالجرائم الإلكترونية، بالإضافة إلى القطاع الخاص والأوساط الأكاديمية والشركاء الآخرين غير العاملين في مجال إنفاذ القانون، ويقوم كذلك بدعم التدريب وبناء القدرات، ولا سيما السلطات المختصة حيث يوفر قدرات دعم جنائية رقمية وتقنية عالية التخصص للتحقيقات والعمليات الاستخبارتية. وهذا المركز مثل مجتمع إنفاذ

[1] Cristos Velasco, Op.Cit, p114.

القانون في الاتحاد الأوروبي في المجالات ذات الاهتمام المشترك فيما يتعلق بمتطلبات البحث والتطوير، وإدارة الإنترنت، وتطوير السياسات خاصة الجنائية[1].

2_ الاورجيست: Eurojust

فعلى المستوى الأوروبي بالإضافة إلى الأوروبول يوجد جهاز أخر، يطلق عليه تسمية الاوروجيست Eurojust وهي وكالة الاتحاد الاوربي للتعاون في مجال العدالة الجنائية، يقع مقرها في لاهاي بهولندا، هدفها مكافحة الإجرام المنظم الخطير العابر للحدود الوطنية[2]، تم تأسيسه بموجب قرار الإتحاد الأوربي رقم JAI/ 187/ 2000 المؤرخ في 28 فبراير 2002 بغرض تقوية التصدي للأشكال الخطيرة للإجرام ومكافحتها[3].

يتمثل دوره في مكافحة جميع أنواع الإجرام، ويؤول له الاختصاص عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى غير عضو في الاتحاد الاوروبي، وتتضمن هذه المنظمة وحدة تعاون قضائي تتمثل مهمتها الرئيسية في التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية[4].

أ_ دور الاوروجيست في مكافحة الجرائم المعلوماتية:

في عام 2019، نشر اليوروبول ويوروجست تقريرًا مشتركًا يحدد ويصنف التطورات الحالية والتحديات المشتركة في مكافحة الجريمة المعلوماتية، والتي تقع في خمسة مجالات مختلفة:

---

[1] أنظر الموقع الرسمي للأوروبول، متوفر على الرابط التالي:
https://www.europol.europa.eu/sites/default/files/documents/ec3_first_year_report.pdf
تم الإطلاع عليه يوم 09/ 06/ 2022 على الساعة08:29.

[2] أنظر الموقع الرسمي للأوروجيست، متوفر على الرابط التالي:
https://www.eurojust.europa.eu./about-us/who-we-are تم الإطلاع عليه يوم 09/ 06/ 2022 على الساعة 11:29.

[3] كعرار سفيان، المرجع السابق، ص577.

[4] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 93.

_ فقدان البيانات: البيانات الإلكترونية هي مفتاح التحقيقات الناجحة في جميع مجالات الجرائم الإلكترونية، لكن إمكانيات الحصول على هذه البيانات كانت محدودة بشكل كبير.

_ فقدان الموقع: أدت الاتجاهات الحديثة إلى وضع قد لا يتمكن فيه تطبيق القانون من تحديد الموقع المادي للجاني أو البنية التحتية الجنائية أو الأدلة الإلكترونية.

التحديات المرتبطة بالأطر القانونية الوطنية: غالبًا ما تثبت الاختلافات في الأطر القانونية المحلية في الدول الأعضاء في الاتحاد الأوروبي أنها عوائق خطيرة أمام التحقيقات الدولية في الجرائم الإلكترونية.

_ عقبات التعاون الدولي: في سياق دولي، لا يوجد إطار قانوني مشترك للتبادل السريع للأدلة (كما هو موجود بالفعل للحفاظ على الأدلة)، كما أن هناك حاجة واضحة إلى آلية أفضل للاتصال عبر الحدود والتبادل السريع للمعلومات.

_ تحديات الشراكات بين القطاعين العام والخاص: يعد التعاون مع القطاع الخاص أمرًا حيويًا لمكافحة الجريمة السيبرانية ، ومع ذلك لا توجد قواعد موحدة للمشاركة ، وبالتالي يمكن إعاقة التحقيقات[1].

ويكمن دور (Eurojust) الأساسي في مكافحة الجرائم المعلوماتية في أنها تساعد الدول الأعضاء في الاتحاد الأوروبي على معالجة الجرائم الإلكترونية من خلال مساعدة المتخصصين في إنفاذ القانون والقضاء على تحديد المتطلبات القانونية لتفعيل التدخلات الضرورية، ومن خلال تسهيل استخدام أدوات التعاون القضائي مثل أمر التحقيق الأوروبي (EIO) ومذكرة التوقيف الأوروبية (EAW).

[1] الموقع الرسمي لليوروجيست، متوفر على الرابط التالي:
https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime
تم الإطلاع عليه يوم 09/ 06/ 2022 على الساعة 12:00.

علاوة على ذلك، تنسق الوكالة التحقيقات عبر الحدود، وضمان الاتصال الفعال ومشاركة الموارد، وتساعد السلطات المعنية على تلبية المتطلبات الفنية للتحقيقات في الجرائم المعلوماتية، والتي قد تشمل التشفير والاحتفاظ بالبيانات وإيجاد حلول للتحديات المتعلقة بحوكمة الإنترنت[1].

فهي تعزز التعاون بين السلطات القضائية المختصة من خلال تمكينها من تبادل الخبرات والمعارف الأخرى ذات الصلة، والممارسات الفضلى فيما يتعلق بالتحقيق والملاحقة القضائية في الجرائم المعلوماتية، وتعزز أيضًا الحوار بين مختلف الجهات الفاعلة وأصحاب المصلحة الذين يلعبون دورًا في ضمان سيادة القانون في الفضاء السيبراني، وتدعم تبادل المعلومات، وتعمل على تطوير عمل السياسات وأنشطة أصحاب المصلحة الآخرين لضمان تفاعل قوي بين خبرة يوروجست في التعاون القضائي الدولي والخبرة التشغيلية والموضوعية لأعضاء الشبكة[2].

ثانيا: التعاون الشرطي على المستوى الافريقي والعربي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تم كذلك تنسق الجهود على المستوى الإفريقي من خلال آلية الإتحاد الإفريقي للتعاون الشرطي لغرض مكافحة مختلف الجرائم بأنواعها التقليدية والمستحدثة، وتم تنسيق الجهود الأمنية كذلك على مستوى الدول العربي من خلال المكتب العربي للشرطة الجنائية لمكافحة.

[1] الموقع الرسمي لليوروجيست، متوفر على الرابط التالي:
https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime
تم الإطلاع عليه يوم 09/ 06/ 2022 على الساعة 12:04.

[2] الموقع الرسمي لليوروجيست، متوفر على الرابط التالي:
https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime
تم الإطلاع عليه يوم 09/ 06/ 2022 على الساعة 12:09.

1_ الافريبول: (آلية الإتحاد الإفريقي للتعاون الشرطي)

رغم أنه لا تزال معدلات ربط افريقيا بالإنترنت هي الأدنى في العالم. ففي عام 2019، لم تتجاوز نسبة سكان القارة الأفريقية الذين يستخدمون الإنترنت 28 في المائة، مقارنة بنسبة 83 في المائة في أوروبا، بحسب أرقام الاتحاد الدولي للاتصالات المشار إليها في تقرير الإنتربول، غير أن هذه المعدلات المنخفضة نسبيا لم تمنع الجماعات الإجرامية المنظمة من استغلال الإنترنت، وتتزايد بإطّراد الجرائم المرتبطة بالبرمجيات الخبيثة في أفريقيا، ففي واحد من بلدان شرق أفريقيا فقط، زادت عن الضِّعف كلفة الاحتيال السيبري بين عامي 2017 و2018، وبلغت قرابة 6,5 ملايين دولار من دولارات الولايات المتحدة[1].

وتستخدم الجماعات الاجرامية المنظمة كذلك وسائل التواصل الاجتماعي لتسهيل جرائم تهريب المهاجرين[2]، وتستخدم أيضا الإنترنت لتسهيل جرائم استغلال الأطفال والاعتداء عليهم جنسيا، وذلك بالاستفادة من الأدوات الرقمية للاتصال بالضحايا واستمالتهم وكذلك لبيع مواد الاستغلال الجنسي للأطفال، والقارة الأفريقية تعتبر أيضا مركز عبور على الصعيد العالمي يتزايد استخدامه للاتجار بالمخدرات وبطائفة واسعة من السلع غير المشروعة، فالمخدرات والمستحضرات الصيدلانية والمركبات الآلية المسروقة وغيرها من البضائع تُباع وتُشترى على الإنترنت بمستوياتها السطحية أو العميقة أو الخفية[3].

---

[1] الموقع الرسمي للانتربول، متوفر على الرابط التالي: https://www.interpol.int/ar/1/1/2020/36 تم الإطلاع عليه بتاريخ 2022/06/10 على الساعة 18:32.

[2] كما يتضح من عملية Sarraounia التي نفِّذت بدعم من الإنتربول وأسفرت عن إنقاذ 232 من ضحايا الاتجار بالبشر في النيجر، من بينهم 46 قاصرا. وكشفت العملية أن 180 ضحية من الذكور قد جُنِّدوا عن طريق رسائل إلكترونية تَعِدهم بإيجاد عمل مناسب.

[3] الموقع الرسمي للانتربول، متوفر على الرابط التالي: https://www.interpol.int/ar/1/1/2020/36 تم الإطلاع عليه بتاريخ 2022/06/10 على الساعة 18:32.

الأفريبول أو منظمة الشرطة الجنائية الإفريقية، بدأت فكرة إنشائها خلال المؤتمر الإقليمي الأفريقي 22 للإنتربول والذي تم في الفترة من 10 إلى 12 سبتمبر 2013 بوهران (الجزائر) والتي شهدت حضور بالإجماع لقادة الشرطة الأفارقة الواحد وأربعون.

بدعوة من الجزائر، عقد المؤتمر الأفريقي للمدراء والمفتشين العامين للشرطة حول الأفريبول يومي 10و11 فيفري2014 ، وقد تمت ترجمة التطلعات المشروعة لمدراء الشرطة إلى واقع من خلال الاعتماد بالإجماع لإعلان الجزائر.

بمناسبة القمة 23 للاتحاد الأفريقي التي عقدت في مالابو في غينيا الاستوائية في الفترة من 20 إلى 27 جوان 2014 تم اعتماد ورقة الجزائر المتعلقة بالأفريبول من قبل قادة ورئساء الحكومات الأفارقة.

أنشئت آلية الاتحاد الافريقي للتعاون الشرطي يوم 13 ديسمبر 2015 في الجزائر، مكونة من قوات الشرطة ل41 دولة، ومقرها الرئيسي بن عكنون بالجزائر العاصمة، وهي منظمة تسهل تبادل المعلومات بين قوات الشرطة الشرطة الوطنية بخصوص الجريمة الدولية والارهاب والاتجار بالأسلحة في افريقيا، هي أكبر منظمة شرطة في القارة الإفريقية[1].

ويتمثل دورها في دعم التعاون الشرطي بين الدول الافريقية من خلال تبادل المعلومات وتعزيز التنسيق بينها، مقرها الجزائر العاصمة وهي مكان إنعقاد دوراتها، ويمكن أن تعقد دوراتها في دول أخرى وذلك بناءا على طلب استضافة يتم تقديمه من طرف الدولة المعنية،

[1] موسوعة ويكيبيديا، متوفر على الرابط التالي :
https://ar.wikipedia.org/wiki/%D8%A3%D9%81%D8%B1%D9%8A%D8%A8%D9%88%D9%84
تم الإطلاع عليه بتاريخ 2022/06/10 على الساعة 16:05.

وتم من خلال النظام الأساسي حصر العضوية في هذه الآلية في الدول الأعضاء في الاتحاد الإفريقي[1].

كجزء من جهود أفريبول لتنفيذ ولايتها، عقد الاجتماع الثاني لفريق العمل المعني بالجرائم الإلكترونية في الجزائر العاصمة، في الفترة من 21 إلى 22 مايو 2019. وكان الهدف الرئيسي للاجتماع هو وضع طرائق لتطوير شبكة من خبراء في منع ومكافحة الجريمة السيبرانية، كعمود فقري للتعاون الشرطي في القارة، ووافق الفريق العامل على طريقة ملموسة للمضي قدما في تنفيذ خطة عمله[2]، مشكلته تمثلت في غياب سياسات (الافتقار للسياسات الضرورية لمكافحة الجريمة السيبرانية)، أفاد التقرير بأن أحد العوامل الرئيسية لتفاقم الجريمة التي يسهل الإنترنت ارتكابها في أفريقيا يتمثل في افتقار العديد من البلدان إلى سياسات واستراتيجيات شاملة لمكافحة الجريمة السيبرية.

ورغم أن الاتحاد الأفريقي قد اعتمد في عام 2014 اتفاقية بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، لم يوقّعها بحلول كانون الثاني/يناير 2020، إلا 14 بلدا من أصل البلدان الـ 55 الأعضاء في الاتحاد الأفريقي.

وتحتاج الاتفاقية إلى مصادقة 15 بلدا عضوا على الأقل لتدخل حيّز النفاذ، وحتى كانون الثاني/يناير 2020، لم تصادق عليها إلا سبعة بلدان.

[1] عبد العزيز لزعر، رشيد زياني، آلية الاتحاد الافريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، كلية العلوم الاجتماعية والإنسانية، جامعة الدكتور مولاي الطاهر سعيدة، الجزائر، المجلد 13، العدد3، سبتمبر 2021، ص254– 255.

[2] الموقع الرسمي للأفريبول، متوفر على الرابط التالي:
https://afripol.africa-union.org/afripol-concludes-the-second-meeting-of-its-working-group-on-cybercrime/?lang=ar
تم الإطلاع عليه بتاريخ 2022/06/10 على الساعة 18:39.

ويفيد التقرير بأن العديد من البلدان الافريقية تعتبر الأمن السيبراني مسألة غير ضرورية[1]، إلا القليل منها.

2_ التعاون الشرطي على المستوى العربي:

أما على المستوى العربي أنشاء مجلس وزراء الداخلية العرب المكتب العربي للشرطة الجنائية بغرض تأمين وتنمية التعاون بين أجهزة الشرطة في الدول العربية الأعضاء في مجال مكافحة الجريمة بكل أشكالها، بما فيها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وملاحقة المجرمين في إطار القوانين والأنظمة المعمول بها في كل دولة، إضافة إلى تقديم المساعدة في مجال دعم وتطوير أجهزة الشرطة في الدول العربية الأعضاء[2].

وما يلاحظ على المستوى العربي دور المكتب العربي للشرطة الجنائية في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات يقتصر على الاعتداءات الواقعة على أنظمة المعالجة الآلية للمعطيات في الاقليم العربي فقط دون تلك العابرة للحدود خارج الاقليم العربي.

المطلب الثاني: التعاون القضائي الدولي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن الهدف الأساسي من هذا التعاون هو تنسيق الجهود على مستوى السلطات القضائية، خلال جميع مراحل الإجراءات القضائية الجنائية، وضمان عدم إفلات المجرم المعلوماتي من العقاب، ويكون ذلك من خلال المساعدة القضائية المتبادلة بن هذه السلطات القضائية (الفرع الأول)، وتسليم المجرمين المعلوماتيين في حالة فرارهم لضمان عدم إفلاتهم من العقاب (الفرع الثاني).

[1] الموقع الرسمي للانتربول، متوفر على الرابط التالي:
https://www.interpol.int/ar/1/1/2020/36
تم الاطلاع عليه بتاريخ 2020/06/10 على الساعة 18:28.

[2] بن مكي نجاة، المرجع السابق، ص150.

الفرع الأول: المساعدة القضائية المتبادلة في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

هناك أشكال معينة من التعاون بين الدول لا يمكن أن تضمنها أجهزة الشرطة أو الآليات التي تستخدم تدابير تدخلية غير إلزامية، على سبيل المثال المساعدة التي تتطلب تدخل السلطات القضائية في الدول التي يتم طلب المساعدة منها، وذلك عندما يتعلق الأمر بالحصول على أمر المحكمة، أو غيرها من الإجراءات الإجبارية للحصول على أدلة في شكل مقبول أو على المعلومات المطلوبة[1].

وتعرف المساعدة القضائية الدولية بأنها "كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم"[2].

وتكون المساعدة القانونية بشأن الحصول على أدلة وأقوال من الأشخاص، أو تبليغ المستندات القضائية، تنفيذ عمليات التفتيش والضبط والتجميد، فحص الأشياء والمواقع، تقديم المعلومات والأدلة والتقييمات التي يقوم بها الخبراء، وتقديم أصول المستندات والسجلات ذات الصلة، بما فيها السجلات الحكومية أو المصرفية أو المالية أو سجلات الشركات أو الأعمال، أو نسخ مصدقة عنها، وتيسير مثول الأشخاص طواعية في الدول الطرف الطالبة، ويمكن أن تتمثل في أي نوع أخر من المساعدة بشرط ألا يتعارض مع القانون الداخلي للدولة الطرف متلقية الطلب[3].

[1] ربيعة فرحي، المساعدة القانونية المتبادلة كآلية للتعاون الدوليالأساس القانوني ومعقوقات التفعيل، مجلة المفكر للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، المجلد 3، العدد4، ديسمبر 2020، ص100.

[2] محمد أحمد سليمان، المرجع السابق، ص 55.

[3] نسيب نجيب، آليات التعاون القانوني الدولي في مكافحة الجريمة المنظمة، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، العدد 1، 2019، ص151-152.

ونصت إتفاقية بودابست على مجالات المساعدة المتبادلة في مجال الجريمة المعلوماتية، حيث تكون المساعدة في مجال الإجراءات الوقتية العاجلة، وفي مجال سلطات التحقيق، وإنشاء طوارئ دائمة لتفعيل المساعدة المتبادلة.

أما بخصوص المساعدة القضائية المتبادلة في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وفقا للتشريع الجزائري:

ورد في نص المادة 16 من القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما أنه بغرض التحريات والتحقيقات القضائية تجرى في مجال الجرائم المتصلة بتكنولوجيات الإعلام الإتصال بغرض كشف مرتكيبيها، يمكن أن يتم تبادل المساعدة القضائية من طرف السلطات المختصة لجمع الأدلة الإلكترونية التي تتعلق بهذه الجريمة، وعند إرسال طلبات المساعدة القضائية المتعلقة بهذه الجرائم بواسطة وسائل الاتصال السريعة كالفاكس أو البريد الإلكتروني وبطبيعة الحال بعد التأكد من صحتها، فإنه يتم قبولها وهذا إذا تعلق الأمر بحالة الإستعجال ويتم مرعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل[1].

وبخصوص تبادل المعلومات واتخاذ الإجراءات التحفظية فإنه تكون وفقا لما ورد في الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل[2].

_ القيود الواردة على طلبات المساعدة القضائية الدولية:

- المساس بالسيادة الوطنية أو النظام العام: حيث يتم رفض تنفيذ طلبات المساعدة القضائية إذا كانت تمس بالسيادة الوطنية أو النظام العام.

[1] أنظر المادة 16 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47، المؤرخة في 25 شعبان عام 1430، الموافق ل16 غشت سنة 2009، ص 8.

[2] أنظر المادة 17 من من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- إمكانية تقييد الإستجابة لطلب المساعدة القضائية بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم إستعمالها في غير ما هو موضح في الطلب[1].

وللمساعدة القضائية عدة أشكال وصور وتتمثل في:

أولا: تبادل المعلومات

يعتبر تبادل المعلومات من أهم أشكال التعاون الدولي في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

فمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات لا تتحقق إلا من خلال تعاون دولي حقيقي، ولا يكون ذلك إلا من خلال التعاون على المستوى الإجرائي، والمتمثل في تبادل المعلومات من خلال تسهيل الإتصال بين الهيئات القضائية بين الدول[2].

يُعرف تبادل المعلومات بأنه "تقديم المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والاجراءات التي إتخذت ضدهم، وقد يشمل التبادل السوابق القضائية للجناة[3]".

ويتم تبادل المعلومات إما بشكل ثنائي أو متعدد الأطراف من خلال الأجهزة المتخصصة في مجال مكافحة مختلف الجرائم المنظمة بصفة عامة والأشكال المستحدثة للإجرام بصفة خاصة وذلك من خلال المنظمة الدولية للشرطة الجنائية (الأنتربول)، أو غيرها من الأجهزة النظيرة على الصعيد الإقيليمي كاليوروبول والأفريبول والمكتب العربي لمكافحة الجريمة، فيتم بين هذه الأجهزة هذا التعاون الدولي الأمني من خلال تبادل

[1] أنظر المادة 18 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 126.

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009، ص407.

المعلومات بين الأجهزة الأمنية حول هذا النوع من الأنشطة الإجرامية التي يباشروها المجرمين المعلوماتيين[1].

والملاحظ أن هذا النوع من التعاون قد تبلور منذ إنشاء المنظمة الدولية للشرطة الجنائية (الانتربول)[2].

ويشمل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية بصدد التحقيق في جريمة ما عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم، كما نصت الاتفاقية الاوروبية لمكافحة الاجرام المعلوماتي في المادة (36/ ب) على ضرورة مشاورة الأطراف فيما بينها حول تبادل المعلومات وكل ما هو جديد في مجال الإجراءات القضائية والجوانب التقنية المتعلقة بمكافحة الجرائم الإلكترونية وجمع الأدلة في الشكل الإلكتروني[3].

ومن المستحسن أن يكون تبادل المعلومات في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال إنشاء قاعدة معطيات بين الدول سواء بشكل ثنائي أو متعددة الأطراف، وإنشاء أنظمة متخصصة لتبادل المعلومات والوثائق إلكترونيا تماشيا مع خصوصية هذه الجريمة التي تتطلب السرعة، إضافة إلى أنها عابرة للحدود الوطنية.

ثانيا: الإنابة القضائية الدولية

1 _ تعريفها:

ويقصد بها طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها، وتهدف هذه الصورة إلى تسهيل

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 75– 77.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 126.

[3] يزيد بوحليط، المرجع السابق، ص359.

الإجراءات الجنائية بين الدول بما يكفل إجراءات التحقيق اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش أو غيرها[1]، وتنفيذ طلب الإنابة غير ملزم بالنسبة للدول المنابة لأن أساسها يقوم على اعتبارات المجاملة الدولية[2].

ويتم إرسال طلب الإنابة القضائية عبر القنوات الدبلوماسية، فمثلا طلب الحصول على دليل إثبات وهو عادة من شأن النيابة العامة تقوم بتوثيقه المحكمة الوطنية المختصة في الدولة الطالبة ثم يمرر بعد ذلك عن طريق وزارة الخارجية إلى سفارة الدولة متلقية الطلب لتقوم هذه الأخيرة بإرساله بعد ذلك إلى السلطات القضائية المختصة في الدولة متلقية الطلب، وما أن يتم تلبية الطلب ينعكس الاتجاه الوارد في سلسلة العمليات، إلا أن هذا الطريق طويل وبطيء، وللحد من البطء والتعقيد يحدث أن تشترط المعاهدات أو الاتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية (وزارة العدل) يتم إرسال الطلبات إليها مباشرة بدلا من الولوج إلى القنوات الدبلوماسية، والتي من شأنها تسريع الإجراءات التي قد تأخذ وقتا طويلا فيما لو تم عبر تلك القنوات.

ولأجل تسريع الإجراءات تم إبرام العديد من الاتفاقيات مثل الاتفاقية الأمريكية الكندية التي تنص على إمكانية تبادل المعلومات شفويا في حال الاستعجال، والمادة 53 من اتفاقية شينغن (1990) والخاصة باستخدام الاتصالات المباشر بين السلطات القضائية في الدول الأطراف، والفقرة 13 من المادة 46 من إتفاقية الأمم المتحدة لمكافحة الفساد[3].

وما يلاحظ هو أن تنفيذ أحكام الإنابة القضائية في المجالات السياسية والضريبية والعسكرية غالبًا ما يتم استبعاده، لأن هذه المجالات من شأنها المساس بالسيادة والنظام

[1] محمد أحمد سليمان، المرجع السابق، ص 56.

[2] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 128.

[3] مناصرة يوسف، المرجع السابق، ص314-315.

العام وبمصالح الدول الأساسية. إلا أن هذا النظام يُعاب عليه أنه يتعلق بالأساليب الدبلوماسية التي تتميز بالبطء والكثير من الشكليات والبروتوكولات التي تتعارض مع طبيعة جرائم البيئة الرقمية التي تتميز بالسرعة والتغيير وأحيانًا تأخر ظهور نتائجها الإجرامية، مما يؤدي إلى ضياع أو اختفاء الأدلة والبيانات، التي قد تشكل أدلة مهمة لإدانة المتهم[1].

2_ شروط تطبيق الإنابة القضائية:

_ لابد من وجود إتفاقيات دولية سواء كانت جماعية أو ثنائية، تسمح باتخاذ السلطات القضائية لإجراءات الانابة القضائية.

_ قيام السلطات القضائية المختصة بإرسال الملف المتعلق بالدعوى الجنائية بكل مرفقاته من مستندات ووثائق ومحاضر التحقيق، والتي تم إجرائها بمعرفة السلطة القضائية في الدولة المطلوب فيها اتخاذ بعض إجراءات التحقيق[2].

ثالثا: نقل الإجراءات

يتمثل نقل الإجراءات في قيام دولة بناء على اتفاقية باتخاذ إجراءات جنائية بصدد جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة، وذلك إذا توافرت شروط معينة منها أن يكون الفعل المنسوب للشخص يشكل جريمة في كلا الدولتين، وأن يؤدي الإجراء المطلوب للوصول إلى الحقيقة، وقد أقرت العديد من الاتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى طرق المساعدة القضائية الدولية كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية، واتفاقية الأمم المتحدة لمكافحة الجريمة عبر الوطنية لسنة 2000، والأمر نفسه نجده في معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي لسنة 1999 بموجب نص المادة 09 منها، وفي الاتجاه نفسه أقر المجلس الأوروبي اتفاقية نقل الإجراءات الجنائية التي تعطي للأطراف المنظمة إمكانية محاكمة الجاني طبقا لقوانينها

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، المرجع السابق، ص 128.

[2] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 78.

بناء على طلب دولة أخرى طرفا في الإتفاقية، بشرط أن يكون الفعل معاقب عليه في الدولتين.

والمشرع الجزائري صادق على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، وابرم الاتفاقيات الثنائية في مجال الجريمة المعلوماتية بقصد التعاون على مكافحتها حيث تم إبرام اتفاقيتين ثنائيتين مع فرنسا الأولى سنة 2007 في مجال التعاون في مكافحة الجرائم المنظمة، والثانية بتاريخ 10/05/ 2016 متعلقة بمكافحة الجريمة المنظمة عبر الأوطان، والجرائم الالكترونية بكافة أشكالها[1].

ويجدر الاشارة إلى أنه توجد العديد من العقبات التي تواجه المساعدة القضائية في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، تتسم إجراءات المساعدة القانونية المتبادلة بالبطء والتعقيد الذي يتعارض مع سرعة الإنترنت وجرائمه، وهو ما ينعكس على ملاحقة مرتكبي جرائم الإنترنت، ضف إلى ذلك بطء الاستجابة في الرد على طلبات المساعدة والرد عليها، وهذا ما يؤثر على العملية[2].

والسبب في ذلك يرجع إما لنقص الموظفين المتدربين في هذا المجال أو بسبب الصعوبات اللغوية أو تباين وإختلاف في كيفية الإجراءات بين الدولتين الطالبة للمساعدة القضائية والدولة المطلوب منها المساعدة القضائية[3].

[1] يزيد بوحليط، المرجع السابق، ص 359-400.

[2] برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية، مجلة البصائر للدراسات القانونية والإقتصادية، كلية الحقوق، جامعة بوشعيب بلحاج عين تموشنت، الجزائر، المجلد 01، العدد01، 2021، ص100.

[3] بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة منتوري قسنطينة، الجزائر، المجلد أ، العدد 50، ديسمبر 2018، ص91.

الفرع الثاني: تسليم المجرمين المعلوماتيين

التسليم هو آلية من آليات التعاون الدولي في مجال الجريمة المعلوماتية، لأن الجريمة المعلوماتية عابرة للحدود الوطنية، وكونها يمكن أن ترتكب في دولة ونتيجتها تتعدى حدود تلك الدولة، والمجرم يمكنه الفرار لدولة أخرى، لذا فإن التسليم بشأنها ضروري، حتى يتم معاقبة الفاعل على فعله الإجرامي.

فمن خلال هذا الفرع سنتطرق إلى تعريف التسليم وشروطه (أولا)، وأسس التسليم في الجريمة المعلوماتية (ثانيا).

أولا: تعريف التسليم وشروطه

1_ تعريفه:

مصطلح التسليم مأخوذ من اللاتينية"extruder"، حيث كان يعبر عنه بإعادة الشخص المطلوب إلى الدولة ذات السيادة والسلطة في محاكمته.

ويُعرف التسليم بأنه إجراء بمقتضاه تقوم الدولة بتسليم شخص موجود في إقليمها لدولة أخرى، تطالب بمحاكمته عن جريمة منسوبة إليه، أو لتنفيذ عقوبة قضت بها عليه محاكم هذه الدولة. وهناك من عرفه بأنه الإجراء الذي تسلم به دولة استنادا إلى معاهدة تأسيسا على المعاملة بالمثل إلى دولة أخرى شخصا تطلبه الدول الأخيرة لاتهامه أو لأنه محكوم عليه بعقوبة جنائية[1].

نص المشرع الجزائري على هذا الإجراء في المواد من المادة 694 إلى 719 من قانون الإجراءات الجزائية الجزائري الواردة في الباب الأول من الكتاب السابع الموسوم ب "تسليم المجرمين".

[1] عفيري عقيلة، عمارة هدى، مبدأ تسليم المجرمين كإجراء لتكريس العدالة الجنائية الدولية، مجلة دراسات وأبحاث المجلة العربية في العلوم الإنسانية والاجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 12، العدد4، 2020، ص 119.

2_ شروطه في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

للتسليم شروط لابد من توافرها حتى يمكن تنفيذه وتتمثل في:

أ_ التجريم المزدوج:

ويقصد بالتجريم المزدوج أن يشكل السلوك الصادر عن الشخص المطلوب سواء كان متهما أو محكوم عليه فعل معاقب عليه في قانون الدولتين، أي يشكل نموذجا إجراميا في التشريعات الجنائية لكلا الدولتين الطالبة والمطلوب منها التسليم، ويخضع للعقوبة المقررة لكل منهما، وبالتالي لا يجوز التسليم إلا إذا كان الفعل المطلوب لأجله التسليم معاقبا عليه كجريمة في كلا الدولتين[1].

لأن الغرض من التسليم هو المحاكمة الجنائية أو تنفيذ العقوبة المقضي بها وفقا لقانون هذه الدولة، ولا محل له إذا انتفى هذا الغرض، ولنفس السبب لا يجوز التسليم لجريمة امتنعت المحاكمة من أجلها لمضي المدة القانونية أو سقطت العقوبة المقضي بها فيها بالتقادم[2].

ب_ عدم جواز تسليم الرعايا:

من بين المبادئ السائدة والمستقرة داخل المجتمع الدولي، والتي تنص عليها معظم التشريعات الوطنية والاتفاقيات الدولية، مبدأ عدم جواز تسليم المجرمين، بغض النظر عن نوع الجريمة التي ارتكبوها في أي إقليم خارج دولتهم[3].

---

[1] علواش فريد، التعاون الدولي عن طريق نظامي تسليم المجرمين والتسليم المراقب، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، المجلد 12، العدد 14، 2017، ص 172-173.

[2] لخضر القيزي، الشروط الموضوعية لتسليم المجرمين، مجلة العلوم الإنسانية لجامعة أم لبواقي، جامعة العربي بن مهيدي أم البواقي، الجزائر، المجلد 07، العدد02، جوان 2020، ص137.

[3] أمير فرج يوسف، الجريمة المنظمة وعلاقتها بالإتجار بالبشر وتهريب المهاجرين غير الشرعيين والجهود الدولية والمحلية لمكافحتها، ط 1، مكتبة الوفاء القانونية، الإسكندرية، 2015، ص79.

وهو شرط من بين الشروط المتعلقة بالأشخاص المطلوب تسليمهم حسب نص المادة 698 الفقرة من قانون إج الجزائري، وهو كذلك مبدأ من المبادئ المستقر عليها في المجتمع الدولي، ولا يهم نوع الجريمة المرتكبة من قبل أحد الرعايا، في أي إقليم خارج دولته، وقياسا على هذا الإجراء لا يجوز تسليم طالبي حق اللجوء السياسي[1].

ج_ عدم جواز تسليم من تمت محاكمته عن ذات الجريمة المطلوب التسليم لأجلها:

فهذا الشرط أحد الضمانات الأساسية للمتهم لأنه يهدف إلى تحقيق أكبر قدر من الحماية القضائية للشخص المطلوب تسليمه، مع ذلك لا يحول دون إمكان إرسال الأجنبي مؤقتا للمثول أمام محاكم الدولة الطالبة على شرط أن يعاد بمجرد الانتهاء من الفصل في الجريمة من طرف القضاء الأجنبي، هذا الشرط يطبق حتى ولو كان الأجنبي خاضعا لإكراه بدني طبقا لنص المادة 701 من ق إج ج[2].

3_ تسليم المجرمين في الاتفاقيات الدولية

أهم الاتفاقيات التي تطرقت إلى مسألة تسليم المجرمين المعلوماتيين تمثلت في إتفاقية بودابست، والاتفاقية العربية.

أ_ تسليم المجرمين في إتفاقية بودابست:

نص الفصل الثاني من إتفاقية بودابست على مبادئ تسليم المجرمين، حيث نصت المادة رقم 24 المُدرجة ضمنه على تسليم المجرمين، ونصت على قابلية هذه المادة للتطبيق بخصوص الالتزام بتسليم المجرمين في الجرائم المنصوص عليها في المواد من المادة 2 إلى المادة 11 من هذه الاتفاقية، والتي تكون معاقب عليها بموجب قوانين الطرفين المعنيين

[1] خرشي عثمان، عمارة فتيحة، تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية، مجلة البحوث القانونية والسياسية، جامعة سعيدة الدكتور مولاي طاهر، الجزائر، المجلد 02، العدد 10، جوان 2018، ص 936.

[2] خرشي عثمان، عمارة فتيحة، المرجع نفسه، ص936.

بعقوبة سالبة للحرية مدتها لا تقل عن سنة أو بعقوبة أشد[1]، وتتمثل هذه الجرائم في الولوج غير القانوني، الاعتراض غير القانوني، الاعتداء على سلامة البيانات، الاعتداء على سلامة النظام، إساءة إستخدام أجهزة الحاسب ومعداته، التزوير المعلوماتي، الغش المعلوماتي، الجرائم المتصلة بالمواد الإباحية للأطفال، الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة، الشروع والاشتراك.

فهذه الجرائم يجب فيها التسليم في كل إتفاقية مبرمة بشأن تسليم المجرمين، أو التي ستبرم بين الأطراف مستقبلا من خلال إدراج هذه الجرائم فيها[2].

وتطبق العقوبة الأقل في الحالة التي يوجد فيها تشريعات موحدة أو متبادلة بالمثل أو بموجب إتفاقية تسليم المجرمين أو بموجب إتفاقية تسليم واجبة التطبيق بين دولتين أو أكثر[3].

في حالة عدم وجود اتفاقية تسليم المجرمين بين الدول الأطراف والتي تجعل التسليم مشروطا بوجود إتفاقية، يمكن اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم بالنسبة للجرائم السالفة الذكر، وبخصوص الدول التي لا تجعل تسليم المجرمين مشروطا باتفاقية تسليم المجرمين، فإنها من خلال مصادقتها على هذه الإتفاقية فإنها تلتزم بها وبالتالي تتبنى الجرائم المنصوص عليها في هذه الاتفاقية كجرائم جائز من أجلها التسليم، ويخضع التسليم لقانون الدولة المطلوب منها التسليم، أو إتفاقية تسليم المجرمين واجبة التطبيق[4]، ويجوز لها رفض التسليم في حالة ما إذا توفرت أسباب رفض التسليم[5]. وفي حالة رفض التسليم في الجرائم السابقة الذكر على أساس الجنسية أو بسبب إنعدام الإختصاص القضائي، يتعين على الدولة المطلوب منها التسليم إحالة الدعوى إلى سلطاتها المختصة

[1] Art 24 de la Convention sur la cybercriminalité.

[2] Art 24 para 2 de la Convention sur la cybercriminalité.

[3] Art 24 para 1 de la Convention sur la cybercriminalité.

[4] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 81.

[5] Art 24 para 5 de la Convention sur la cybercriminalité.

وإبلاغ طرف الدولة الطالبة بالنتيجة، وتقوم الدول عند التوقيع بإخطار السكريتير العام لمجلس أوروبا باسم السلطة المسؤولة عن طلبات التسليم[1].

وتقوم الدول الأطراف عند التوقيع، أو التصديق، أو القبول أو الموافقة على الإنضمام لإتفاقية بودابست بإخطار السكريتير العام لمجلس أوروبا بإسم السلطة المسؤولة عن طلبات التسليم سواء أرسلتها أو إستلمتها أو القبض المؤقت، ويقوم السكريتير العام لمجلس أوروبا بإنشاء سجل ليدون فيه هذه البيانات، وتقوم الدول الأطراف بالتأكد من البيانات المدونة في هذا السجل[2].

ب_ تسليم المجرمين في الإتفاقية العربية:

نصت المادة 31 من الإتفاقية العربية على تسليم المجرمين حيث أن الدول الأطراف في هذه الاتفاقية يمكنهم الإعتماد عليها وإعتبارها أساس قانوني لعملية تسليم المجرمين، وضبطت شروط التسليم حيث أن الجرائم التي يجوز فيها التسليم لا تقل عقوبتها عن سنة أو أكثر، ووجوب تطبيق الشروط المنصوص عليها في قانون الدولة المقدم إليها طلب التسليم، ضف إلى ذلك أن هذه المادة قررت حق الدول الأطراف في رفض التسليم مع تعهد هذه الدول بتوجيه الاتهام للجناة الذين يرتكبون جرائم معاقب عليها بموجب قانون الدولتين بعقوبة لاتقل عن سنة أو بعقوبة أشد لدى أي من الدولتين[3].

ثانيا: أسس التسليم في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

من أسس التسليم أن الدول لا تلتزم بالتسليم إلا إذا كان بناء على معاهدات دولية أو على أساس المعاملة بالمثل.

[1] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 81.

[2] Art 24 para 7 de la Convention sur la cybercriminalité.

[3] رامي متولي القاضي، عمر سالم، المرجع نفسه، ص 82.

1_ المعاملة بالمثل:

وتُعرف المعاملة بالمثل في مجال تسليم المجرمين والعلاقات الدولية بأنها تطابق الحقوق والالتزامات أي التزام كل دولة في مواجهة دولة أخرى بمجموعة من الحقوق والالتزامات التي يفرضها عليها حسن تطبيق هذا المبدأ، ويلزم كل منها بتطبيقه في المستقبل، وتعتبر المعاملة بالمثل من المسائل الهامة والمعاصرة في مجال العلاقات الدولية والمسائل الجنائية[1].

2_ المعاهدات الدولية:

وتمثل المعاهدات أهم أدوات التعاون الدولي لأنها تعبر صراحة عن نية أطرافها لتحقيق هذا الإطار المتعاون فيما ينظمه موضوع المعاهدة، ولهذا فإن مصدر نظام تسليم المجرمين في معظم البلدان أساسه المعاهدات والاتفاقيات الدولية سواء كانت متعددة الأطراف أو ثنائية[2].

في حالة غياب إتفاقية تسليم بين دولتين ولم يكن لدى إحداهما تشريع داخلي ينظم مسألة التسليم، فإن الالتزام القانوني للتسليم بخصوص الجرائم يجد مصدره في الإتفاقية المنظمة لأحكام التسليم بخصوص جريمة معينة[3].

من أهم الاتفاقيات للتعاون الدولي في مجال الإجراءات الجنائية عامة لمكافحة الجرائم الناشئة عن استخدام الحاسوب والانترنت، اتفاقية بودابست بتاريخ 23 نوفمبر 2001، التي أجازت تسليم المجرمين في الجرائم المعلوماتية في المواد من 2 إلى 11 من الاتفاقية.

[1] جيلالي الحسين، المرجع السابق، ص 23.

[2] محمد أحمد عبد الرحمن طه، النظام القانوني لتسليم المجرمين مصادر وأنواع التسليم، دراسات قانونية، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، الجزائر، العدد7، ماي 2010، ص 88.

[3] سارة محمد، التعاون الدولي في تسليم المجرمين في ضوء التشريعات الوطنية والاتفاقيات الدولية، مجلة جامعة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد17، العدد 1، يونيو 2020، ص656.

وعقدت كذلك الجزائر في مجال التعاون القضائي وتسليم المجرمين عدة اتفاقيات ثنائية مع: المغرب في مارس 1963، وتونس في 14 نوفمبر 1963، وجمهورية مصر العربية في 29 جويلية 1965، فرنسا في 14 أكتوبر 1966، موريتانيا في 15 جانفي 1970، بلجيكا في 8 أكتوبر 1970، ألمانيا الديمقراطية في 21 نوفمبر 1973، كوبا في أوت 1990.

وعليه فالمعاهدات والاتفاقيات تعد المصدر الأول والأصيل للتسليم خاصة في مجال مكافحة الجرائم المعلوماتية[1] يستند تسليم المجرمين إلى اتفاقيات، سواء كانت ثنائية أو متعددة الأطراف التي تنظم القواعد المطبقة بين الأطراف المتعاقدة في مسائل تبادل تسليم المجرمين أو استرداد المجرمين، سواء تمت محاكمتهم أم مازالوا في طور الملاحقة لم تصدر عليهم أحكام[2].

فهذه المعاهدات تنظم شروط التسليم وتحدد حالاته وإجراءاته والجرائم التي يجوز فيها التسليم والتي لا يجوز فيها التسليم، فهدف هذه الاتفاقيات تحسين التعاون، وتتضح أهمية هذه المعاهدات في مجال لتسليم المجرمين من واقع التزام الدولة بما ورد فيها من نصوص واعتماد الدولة الطالبة عليها كسند قانوني تستند عليه عند تقديم طلبها يكون ملزما لهما عند إجراء التسليم[3].

وما تجدربنا الإشارة إليه في هذا الصدد هنا إلى أنه بينما تتمتع الاتفاقات والمعاهدات الدولية بامتيازات وقوة ملزمة من جانب الدول الأطراف، تتعرض هذه الاتفاقيات إلى عقبات

[1] خرشي عثمان، عمارة فتيحة، المرجع السابق، ص 932 -933.

[2] برقوق يوسف، المرجع السابق، ص97.

[3] محمد أحمد عبد الرحمان طه، المرجع السابق، ص88.

بسبب تعارضها، سواء مع التشريعات المحلية أو مع الاتفاقيات أو المعاهدات الأخرى، ولكن في هذه الحالة الأخيرة، نصت بعض الاتفاقيات على حل وسط لهذه المسألة، على سبيل المثال، تنص المادة 18 من إتفاقية جامعة الدول العربية لتسليم المجرمين على أنه في حالة تعارض أحكام هذه الاتفاقية مع أحكام أي من الاتفاقيات الثنائية التي تربط هذين الدولتين، فإنهما تطبقان الأحكام الأكثر تيسيرًا لتسليم المجرمين[1].

3_ القوانين الداخلية:

لا شك أن القوانين الوطنية تعكس صورة الالتزامات الدولية، وتعتمد العديد من الدول على تنظيم شروط التسليم في القانون الداخلي لها، وتعتبره مصدر أصلي لإجراءاته وأحكامه القانونية، ويتصدر التشريع الفرنسي الصادر في العاشر من مارس سنة 1927 قائمة التشريعات الأوروبية في مجال تسليم المجرمين[2].

لا شك أن القوانين الوطنية تعكس الالتزامات الدولية، وتعتمد العديد من الدول على تنظيم شروط التسليم في قانونها الوطني وتعتبره المصدر الأصلي لإجراءات التسليم، بما في ذلك النظام الأنجلو أمريكي. ويستند إلى قانون تسليم المجرمين لعام 1989 وهذا التشريع آخذ في التطور، وفي 10 مارس 1927 نشرت فرنسا قائمة بالتشريعات الأوروبية المتعلقة بتسليم المجرمين.

[1] سارة محمد، المرجع السابق، ص 657.

[2] محمد نصر القطري، آليات التعاون الدولي لتسليم المجرمين وآثاره في الحد من الجرائم المستحدثة، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 35، العدد3، 2019، ص407.

وما يجدر بنا الإشارة إليه في هذا الصدد أنه بالنسبة للدول التي لا يوجد بها قانون وطني يتضمن قواعد وإجراءات تسليم المجرمين فإنها تعتمد على الإتفاقيات الثنائية ومتعددة الأطراف كمصدرا أساسيا له[1].

وبالنسبة للتشريع الجزائري لا يوجد قانون وطني داخلي خاص بتسليم المجرمين وإنما تم تنظيم أحكام التسليم في قانون الإجراءات الجزائية الجزائري ضمن الباب الأول من الكتاب السابع تحت عنوان "تسليم المجرمين" والذي تضمن 27 مادة من المادة 694 إلى غاية المادة 720 من قانون الإجراءات الجزائية الجزائري.

وهذا الباب تم تقسيمه إلى خمسة فصول عُنون الفصل الأول بشروط تسليم المجرمين من المادة 694 إلى المادة 701. أما الفصل الثاني فعُنون بإجراءات تسليم المجرمين من المادة 702 إلى المادة 713، أما الفصل الثالث فعُنون بآثار التسليم من المادة 714 إلى المادة 718. والفصل الرابع عنون ب: في العبور(الترانزيت) تضمن المادة 719، أما الفصل الأخير فعُنون ب: في الأشياء المضبوطة وتضمن كذلك مادة وحيدة وهي المادة 720 منه.

وما يلاحظ هو عدم كفاية التعاون الدولي في مجال التسليم في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وذلك لعدم وجود اتفاقيات دولية كافية لتسليم المجرمين أو التعاون سواء كانت ثنائية أو جماعية بين الدول تسمح بالتعاون الدولي، أو عدم كفايتها إن وجدت، للتصدي للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات نظرا لمتطلباتها الخاصة وكذا مرونة وتطور البحث والتحري عنها وذلك لضمان سرعتها[2].

[1] محمد نصر القطري، المرجع السابق، ص407.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص87.

خلاصة الباب الأول:

تم إنتهاج سياسة جنائية دولية خاصة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ولتجسيد هذه السياسة تم الإعتماد على العديد من الآليات على المستوى الموضوعي تمثلت في الجهود الدولية التي كانت بمثابة إرهاصات مهدت لبلورة تشريعات دولية لمكافحتها على المستويين الدولي والإقليمي، من خلالها تم إيجاد تشريعات دولية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بصفة عامة، وتشريعات دولية خاصة بحماية المعطيات الشخصية، وجسدت هذه التشريعات الدولية المتعددة الأطراف سياسة جنائية تشريعية مشتركة.

وإجرائيا تم التوجه نحو اعتماد مبدأ الاختصاص الجنائي العالمي، باعتبار هذه الجرائم من أشد الجرائم خطورة كونها تقع في الفضاء السيبراني المعنوي اللامحدود جغرافيًا، المتضمن الدليل الرقمي، الذي يصعب إثباته وكشفه من الجهات القضائية المعنية، لسهولة وسرعة حذفه، وبالتالي تصعب عملية القبض على الجناة لعبور الجريمة الحدود الوطنية، لذا فهي تفرض ضرورة التعاون بين الدول لأجل مكافحتها، ومن أهم آليات التعاون الدولي: التعاون القضائي الذي يكون من خلال التعاون الشرطي الدولي، والمساعدة القضائية بكافة صورها وأشكالها من تبادل المعلومات، نقل الإجراءات والإنابة القضائية والمساعدة القضائية، أضف إلى ذلك التسليم والذي من خلاله يصعب على المجرم المعلوماتي الفرار، ويتم توقيع العقاب عليه.

الباب الثاني: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الباب الثاني: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تطرقنا في الباب الأول إلى السياسة الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على الصعيد الدولي، التي تجسدت من خلال عدة آليات أهمها الآليات الإتفاقية على المستوى الإقليمي والدولي.

فالدول الأطراف في مختلف الاتفاقيات الدولية السابقة الذكر تلتزم بأن تكيف قوانينها الداخلية بما يجعلها متلائمة مع الأحكام الواردة في تلك الاتفاقيات، أو تشرع قوانين جديدة بغرض ضمان التوافق بين تشريعاتها الداخلية وأحكام هذه الاتفاقيات، وهذا الالتزام يعتبر التزام جوهري فرضته قاعدة الوفاء بالعهود كأصل عام، وبالفعل فإن تطبيق هذا الالتزام في المسائل الجزائية يثري ويطور القواعد القانونية الداخلية في مختلف الأنظمة القانونية الداخلية، وتتجسد من خلاله فعالية هذه الاتفاقيات[1].

وعليه انتهج المشرع الجزائري سياسة جنائية على المستوى الموضوعي والإجرائي لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وذلك وفقا لمقتضيات السياسة الجنائية المعاصرة وكذلك تماشيا مع الصكوك والمواثيق الدولية التي صادقت عليها الجزائر من خلال موائمة تشريعاتها الوطنية مع ما ورد في التشريعات الدولية، سواء في الجانب الموضوعي أو الجانب الإجرائي لهذه التشريعات.

[1] العنكبي نزار، المرجع السابق، ص 80 – 81.

الفصل الأول: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الموضوعي

إن الشق الموضوعي للسياسة الجنائية يتعلق بالتجريم والعقاب، وكلاهما يخضع لمبدأ الشرعية الجنائية المنصوص عليه بموجب المادة 1 من قانون العقوبات الجزائري.

المشرع الجزائري وبغرض مكافحة هذا النوع المستحدث من الإجرام، أضفى حماية جنائية موضوعية لأنظمة المعالجة الآلية للمعطيات من جميع الجوانب بغرض الإحاطة بهذه الأفعال المجرمة وتطويقها، فأقر حماية جنائية للنظام في حد ذاته وذلك بموجب قانون العقوبات الجزائري، من خلال تجريم السلوكات الإجرامية الواقعة على هذا النظام في حد ذاته، ومكوناته المادية والمنطقية، وكذلك جرم الأفعال التي يكون فيها النظام ليس هو محل الاعتداء وإنما يتم استخدامه كوسيلة لارتكاب أفعال إجرامية، وكذلك أقر من خلاله بحماية معطيات النظام بكل أنواعها، لكن حماية هذه المعطيات لم تكن كافية بموجب قانون العقوبات وذلك لكثرت الاعتداءات على المعطيات ذات الطابع الشخصي والمساس بالحياة الخاصة، فتم وضع تشريع خاص يحمي هذا النوع من المعطيات.

من خلال هذا الفصل سنتطرق إلى السياسية التجريمية والعقابية التي اتبعها المشرع الجزائري لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الأول)، السياسة التجريمية والعقابية التي اتبعها المشرع الجزائري لمكافحة جرائم المعطيات الشخصية (المبحث الثاني).

المبحث الأول: السياسية التجريمية والعقابية التي اتبعها المشرع الجزائري لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تنقسم الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات إلى قسمين منها الجرائم الواقعة على النظام في حد ذاته ومنها الجرائم الواقعة بواسطة النظام أو النظام يسهل ارتكابها عن طريق الأنترنت، لذا من خلال هذا المبحث سنتطرق إلى الجرائم التي تكون فيها أنظمة المعالجة الآلية للمعطيات هدفًا، والتي أطلق عليها المشرع الجزائري تسمية جرائم المساس بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، الجرائم الواقعة باستخدام أنظمة المعالجة الآلية للمعطيات (المطلب الثاني).

المطلب الأول: مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

نص المشرع الجزائري في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15 المؤرخ في نوفمبر 2004، فتضمن هذا القسم المواد من 394م كرر إلى 394 مكرر07، أي تضمن سبعة مواد، وجرم مختلف الأفعال الاجرامية التي تمس بهذه الأنظمة[1]، وبموجب القانون رقم 16-02 المؤرخ في 19 يونيو سنة 2016 أضاف المشرع المادة 394 مكرر 08 لهذا القسم.

[1] زراري نسرين، بوقرة اسماعيل، نحو التحول إلى المحكمة الرقمية، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، المجلد 10، العدد 02، 2023، ص459.

الفرع الأول: جريمة الدخول والبقاء غير المشروع

تعتبر جريمتي الدخول والبقاء غير المشروع من أخطر جرائم المساس بأنظمة المعالجة الآلية للمعطيات، لأنه قد ينتج عن سلوك الدخول أو البقاء في نظام المعالجة الآلية للمعطيات بطريقة غير مشروعة يتم المساس بنظام المعالجة الآلية والمساس بمعطياته، التي تعتبر جرائم معلوماتية بَحْتَة كما يطلق عليها.

فالمشرع الجزائري جرم مجرد الدخول إلى نظام المعالجة الآلية للمعطيات، ولو لم يترتب عليه أي نتيجة إجرامية، وجرم كذلك البقاء الذي يكون نتيجة الدخول غير المشروع، والبقاء الذي يكون منفصل عن جريمة الدخول غير المشروع، أي الذي يكون نتيجة دخول مشروع لكن المُجْرِم بقي في النظام.

ومن خلال هذا الفرع سنتطرق إلى جريمة الدخول عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات (أولا)، جريمة البقاء غير المشروع في الأنظمة المعلوماتية (ثانيا).

أولا: جريمة الدخول عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات

اختلفت تسميات هذه الجريمة، وتنوعت الدلالات المستخدمة في التعبير عن الفعل الذي تتحقق به هذه الجريمة، فمنهم من استخدم مصطلح الدخول إلى النظام الآلي، ومنهم من استخدم مصطلح الولوج إذا كان هذا الدخول إلكتروني، ومنهم من استخدم انتهاك نظام المعلومات، ومنهم من عبر عنها باختراق النظام الآلي[1]، أما المشرع الجزائري استعمال مصطلح الدخول عن طريق الغش إلى منظومة للمعالجة الآلية للمعطيات.

[1] محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها– دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني–، دار الكتاب القانوني، دار شتات للنشر والبرمجيات، 2014، ص 234– 235.

1_ الركن المفترض:

فنظام المعالجة الآلية للمعطيات يشكل أساس التجريم الذي اعتمده المشرع[1]، إذ يعتبر ركن مفترض، وبدونه لا تقوم جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات، لأنه في غياب هذا النظام لا يكون هناك مجال للبحث في مدى توافر أركان جرائم المساس بأنظمة المعالجة الآلية للمعطيات[2]، فمحل الجريمة هو منظومة للمعالجة الآلية للمعطيات أو جزء منها، وتجدر الإشارة أن المشرع الجزائري لم يحدد مفهوم نظام المعالجة الآلية للمعطيات ومكوناته، حيث لم يورد له تعريف في قانون العقوبات، وحذا حذو المشرع الفرنسي في هذا الصدد[3] الذي ترك مهمة تعريفه للفقه والقضاء وهذا يرجع إلى خضوع هذا النظام للتطورات السريعة والمتتالية التي تتماشى مع التطور التكنولوجي[4].

لكنه في سنة 2009 تم تعريفه من قِبل المشرع الجزائري حيث تدارك ذلك وعرف المنظومة المعلوماتية من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها في المادة 02 منه التي نصت على أن" منظومة معلوماتية: أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[5]، وما يلاحظ على هذا التعريف أنه تقني أكثر من أنه قانوني وجاء غامض لا يحدد العناصر المكونة لهذا النظام والتي يمثل الدخول اليها هذه الجريمة.

---

[1] Guillaume champy, La Fraude Informatique, T1 , presses universitaires d'aix-marseille , marseille ,1992 , P370.

[2] خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، د. ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2010، ص 108.

[3] فلم يرد تعريف رسمي لنظام المعالجة الآلية للمعطيات في القرار المتعلق بإثراء المصطلحات المعلوماتية الفرنسي رغم أنه يمثل أساس النظرية العامة للقانون المعلوماتي. للتفصيل أكثر أنظر: محمد خليفة، المرجع السابق، ص 26.

[4] زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، د. ط، المنشورات الحقوقية صادر، بيروت، لبنان، د. س. ن، ص 32.

[5] أنظر المادة 02 من القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

2_ الركن الشرعي: نصت المادة 394 مكرر من ق ع ج على أنه يتم معاقبة كل من يدخل أو يحاول الدخول عن طريق الغش إلى منظومة معالجة آلية كاملة أو جزء منها[1].

وهو نفس السلوك المجرم المنصوص عليه في ق ع ف[2].

3_ الركن المادي للجريمة:

إن السلوك الإجرامي لهذه الجريمة يتمثل في الدخول إلى كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك، وهذا السلوك هو سلوك إيجابي يتمثل في حركة إرادية من شأنها إحداث أثر ملموسا في العالم المعلوماتي الرقمي[3].ولم يورد المشرع الجزائري تعريفا للدخول مثلما فعلت غالبية التشريعات والتي نذكر منها على سبيل المثال، نظام مكافحة جرائم المعلوماتية السعودي[4]، واشترط المشرع الجزائري أن يكون الدخول إلى نظام المعالجة الآلية عن طريق الغش، أو التحايل ومن ثمة النفاذ والوصول إليه. فيبدو من خلال وجود عبارة الغش أو التحايل أنه يتطلب أن يكون النظام محميًا بوسائل فنية أو تقنية[5]، وهذا يتنافى مع نية المشرع الجزائري، حيث أن هذا الأخير لم يشترط مثل بعض التشريعات ضرورة حماية نظام المعالجة الآلية تقنيًا أو فنيًا.

---

[1] أنظر المادة 394 مكرر من القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج. ر.ج .ج، العدد 71، المؤرخة في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

[2] نص عليها ق.ع. ف بموجب المادة 323-1 ، والملاحظ أن كلا من المشرع الجزائري والفرنسي جرم مجرد الدخول إلى نظام المعالجة الآلية، وهذه الجريمة أطلق عليها كل من المشرع الجزائري والمشرع الفرنسي نفس التسمية والمتمثلة في "جريمة الدخول إلى النظام الآلي لمعالجة المعطيات عن طريق الغش".

[3] محمد خليفة، المرجع السابق، ص 139.

[4] المادة (7/2) نظام مكافحة جرائم المعلوماتية السعودي، رقم 17 الصادر بتاريخ 03/26/ 2007، الجريدة الرسمية، مجموعة الأنظمة السعودية، الذي عرف الدخول غير المشروع بأنه " دخول شخص بطريقة متعمدة إلى الحاسب الآلي، أو موقع إلكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها"

[5] محمد حماد مرهج الهيتي، المرجع السابق، ص 234.

وأورد المشرع الجزائري عبارة "الدخول" غير محددة وغير مضبوطة، وشاملة تتسع هذه العبارة لتشمل جميع تقنيات وطرق الدخول الاحتيالي غير المشروع في منظومة معلوماتية محمية أو غير محمية[1]، ويتم في حالة عدم وجود تصريح أو إذن، ولم ينص المشرع الفرنسي على انتهاك أدوات ووسائل الحماية وقت الدخول، وبالتالي يبقى هذا الأمر حسب تقدير القاضي[2]، مثله مثل المشرع الجزائري.

ولم يحدد المشرع الجزائري وسيلة محددة للدخول، لكنه لم ينص على ذلك صراحة في نصوصه التشريعية، كما فعلت معظم التشريعات المقارنة، ومنها على سبيل المثال القانون الأردني[3]، وكذلك القانون القطري[4].

والدخول يكون بطريقتين: الأولى تتمثل في الدخول المباشر إلى نظام المعالجة الآلية للمعطيات أي الإتصال المادي المباشر من خلال الدخول إلى النظام دون الحاجة إلى شبكة إتصال معلوماتية حتى تُرتكب الجريمة، ففي هذه الحالة يكون الجاني في نفس موقع النظام

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، ط 21، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2019، ص435.

[2] حيث صدر قرار عن مجلس قضاء باريس بأن جريمة الدخول غير المشروع تُرتكب حتى في غياب وسائل الحماية التقنية، وعليه تقوم الجريمة بمجرد الدخول البسيط بدون حق، وهذا ما قرره إليه القضاء الجزائري بشأن الفصل في مسألة مدى إشتراط تأمين النظام المعلوماتي لوقوع جريمة الدخول غير المشروع، من خلال القرار الجزائي لمجلس قضاء الجزائر، الصادر عن الغرفة الجزائية الثالثة، رقم الفهرس: 16/ 09247، الصادر بتاريخ 2016/06/27، الغير منشور. مناصرة يوسف، المرجع السابق، ص 124- 125.

[3] المادة (1/3) من قانون الجرائم الإلكترونية الأردني، رقم 27 لسنة 2015، المنشور على الصفحة 5631، من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1 التي نصت على أن: " كل من دخل قصدًا إلى موقعٍ إلكتروني، أو نظام معلومات **بأي وسيلة** بدون تصريح..."

[4] تنص المادة 3 من قانون رقم (14) لسنة 2014، المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، الصادر بتاريخ 2014/09/15 الموافق 11/20/ 1435، الجريدة الرسمية القطرية العدد 15، الصادرة بتاريخ 2014/10/02 الموافق 1435/12/08 على أنه: " يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة لا تزيد على (500,000) خمسمائة ألف ريال، كل من دخل عمدا، دون وجه حق، **بأي وسيلة**، موقعا إلكترونيا، أو نظاما معلوماتيا، أو شبكة معلوماتية، أو وسيلة تقنية معلومات أو جزء منها، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك..."

محل الجريمة، أما الطريقة الثانية تتمثل في الدخول غير المباشر لنظام المعالجة الآلية للمعطيات ويطلق عليه كذلك تسمية الإتصال المعنوي ويتم من خلال إستخدام وسائل الاتصال عن بعد المستحدثة (كالشبكات المعلوماتية السلكية أو اللاسلكية)[1]، وبالتالي يستنتج أن معيار التفرقة بين هذين النوعين يتمثل في الوسيط الإلكتروني و تواجد الجاني في نفس المكان المتواجد به النظام محل الجريمة.

وخلافا للمشرع الجزائري هناك من التشريعات التي حددت محل جريمة الدخول غير المشروع إلى النظام المعلوماتي، وحصرته في الدخول لمجموعة من العناصر ولم يقتصر على الدخول إلى نظام المعالجة الآلية للمعطيات فقط، ومثاله المشرع الإمارتي وذلك بموجب المادة 2 [2] منه الذي حددها كما يلي[3]: الموقع الإلكتروني[4]، ونظام المعلومات الإلكتروني[5]،

[1] عز الدين عثماني، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، المجلد 09، العدد 03، ديسمبر 2018، ص 616.

[2] المادة 02 من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات تنص على أنه: " يعاقب بالحبس والغرامة التي لا تقل عن مائة ألف درهم ولا تزيد عن ثلاثمائة درهم، أو بإحدى هاتين العقوبتين كل من دخل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة..."

[3] إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، كلية القانون، نوفمبر 2018، ص 12.

[4] المادة 01 من مرسوم بقانون رقم (5) لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون، بتاريخ 26-8-2012، الإمارات العربية المتحدة عرفت **الموقع الإلكتروني**: مكان إتاحة المعلومات إلكترونية على الشبكة المعلوماتية ومنها مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات

[5] المادة 01 من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، عرفت "**نظام المعلومات الإلكتروني**: مجموعة برامج معلوماتية ووسائل تقنية المعلومات المعدة لمعالجة وإدارة وتخزين المعلومات الإلكترونية أو ما شابه ذلك".

شبكة المعلومات[1]، وسائل تقنية المعلومات[2]، وهذا خلافا للمشرع المصري[3]، الذي نص على أن الموقع أو الحساب الخاص لا يندرج ضمن أجزاء النظام المعلوماتي.

4_ الركن المعنوي:

الركن المعنوي في جريمة الدخول غير المشروع يأخذ شكل القصد الجنائي بعنصريه العلم والإرادة، فالجاني يعلم أن دخوله إلى نظام المعالجة الآلية أو جزء منه، وهذا النظام خاص بالغير، وأنه لا يحق له الدخول إليه، وأن إرادته تتجه إلى ارتكاب هذا السلوك الإجرامي، وبالتالي فهذه الجريمة لا تقوم في حالة غياب القصد بعنصريه وكانت عن طريق الخطأ كما لو توصل شخص بالصدفة أو عن طريق الخطأ إلى نظام معلوماتي لكن بشرط خروجه فور علمه بذلك، لأنه إذا استمر في البقاء داخل هذا النظام وانصرفت ارادته لذلك تقوم مسؤوليته الجنائية عن جريمة أخرى مستقلة وهي البقاء غير المشروع والتي سنفصل فيها لاحقا[4]. وكذلك اشترط المشرع الجزائري في هذه الجريمة قصدًا جنائيًا خاصا يتمثل في نية الغش، وتتوافر هذه النية عندما يعلم الجاني المعلوماتي أنه ليس له حق الدخول في نظام المعالجة الآلية للمعطيات، وتُشترط كذلك سواء تم الدخول أو لم يتم، ولا يهم إن تم

[1] المادة 01 من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، عرفت "ال**شبكة المعلوماتية:** إرتباط بين مجموعتين أو أكثر من البرامج المعلوماتية ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات"

[2] المادة 01 من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، عرفت " **وسيلة تقنية المعلومات:** هي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للأخرين".

[3] نصت المادة 14 من القانون رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر (ج)، الصادرة بتاريخ 14 أغسطس سنة 2018 على أنه " يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول اليه"

[4] زينات طلعت شحادة، المرجع السابق، ص 51- 52.

المساس بالمعطيات في حد ذاتها أم لا من خلال تحقق نتيجة معينة تتمثل في الحذف أو التغيير لمنظومة المعطيات أو لم تتحقق إذا تم الدخول[1].

5_ العقوبات:

عقوبة جريمة الدخول عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات في صورتها البسيطة هي:

بالنسبة للشخص الطبيعي هي الحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج إلى 300.000 دج حسب ما نصت عليه م 394 مكرر من ق.ع .ج.

بالنسبة للشخص المعنوي: يعاقب بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[2].

ويتم تطبيق نفس العقوبات المذكورة أعلاه على الشخص الطبيعي والمعنوي في حالة المحاولة[3]، وكذلك بالنسبة للمشاركة أو إتفاق لأجل الاعداد لجريمة لهذه الجريمة، وتجسد هذا التحضير بفعل مادي[4].

وتجدر الإشارة إلى أنه يُحكم بالمصادرة كعقوبة تكميلية في هذه الجريمة، والمصادرة تتمثل في نزع ملكية المال قسْرًا على مالكه وإضافته إلى ملك الدولة بدون مقابل[5]، وتكون هذه المصادرة على جميع الأجهزة والبرامج وكل الوسائل المستخدمة في الجريمة، وإغلاق

[1] حديدان سفيان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 2، العدد 8، ديسمبر 2017، ص 676.

[2] أنظر المادة 394 مكرر 4 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[3] أنظر المادة 394 مكرر 7 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[4] أنظر المادة 394 مكرر5 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[5] محمد سيد عبد الوهاب أبو سريع وشهرته، محمد أبو الخير، الدفوع الجنائية في جرائم الأنترنت (الجرائم الالكترونية)، الكتاب الثاني، ط1، دار المحامي للإصدارات القانونية، ، د. ب. ن، 2022، ص 153.

المواقع المعتمدة فيها، بالإضافة إلى إغلاق مكان الاستغلال مع مراعاة حقوق الغير حسن نية وعدم الإخلال بها[1].

ثانيا: جريمة البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات

أورد المشرع الجزائري هذه الجريمة في المادة 394 مكرر من قانون العقوبات الجزائري مع جريمة الدخول عن طريق الغش إلى المنظومة المعلوماتية أو جزء منها، مقررًا لهما نفس العقوبة الجزائية، وحذا حذو المشرع الفرنسي الذي أوردهما في نفس المادة 1/323 وقرر لهما نفس الجزاء.

1_ الركن المفترض: يتمثل في وجود نظام معالجة آلية للمعطيات، سبق وأن تم التفصيل فيه.

2_ الركن المادي

والركن المادي لهذه الجريمة يتمثل في فعل البقاء غير المشروع في نظام المعالجة الآلية للمعطيات والذي يُعرف على أنه "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام". فالبقاء يتمثل في عدم قطع الفاعل تواصله وارتباطه بالنظام عندما يدرك أن وجوده فيه غير مشروع، وبالتالي فهو يبدأ من الوقت الذي كان يجب أن يغير فيه الشخص وضعه بمغادرة النظام[2]، ويتمثل كذلك في كل تواجد يتم من خلال الاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي[3]، ويمكن أن يتخذ النشاط الإجرامي في هذه الجريمة عدة صور الأولى تتمثل في التواجد داخل نظام معالجة البيانات

[1] أنظر المادة 394 مكرر6 من القانون رقم 15- 04 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[2] محمد خليفة، المرجع السابق، ص 154.

[3] أحمد بن مسعود، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 10، العدد1، 2017، ص 485.

الآلي ضد إرادة صاحب النظام أو من يتحكم فيه تكون دون إذن أو ترخيص، فالسلوك المجرم يكون تام بمجرد دخول النظام والبقاء فيه، وقد جمع المشرع هذين السلوكين بالغش (Frauduleusement)، لذلك في هذه الحالة فإن جريمة البقاء هي تالية للدخول غير المشروع[1]، وقد يتم الجمع بينهما في نفس الوقت ففي هذه الحالة يتحقق الإجتماع المادي للجريمتين معًا[2]، أما الصورة الثانية يكون فيها البقاء معاقبا عليه مستقل عن الدخول إلى النظام ففي هذه الحالة يكون سلوك الدخول إلى النظام مشروعا[3]، فيكون التواجد فيه بناءً على إذن أو تصريح من صاحبه أو المتحكم فيه، ولكنه لا يغادره بعد دخوله، وكذلك في الحالة التي يكون فيها الدخول صدفة وليس عمدًا، في هذه الحالة يجب على الفاعل الخروج والانسحاب فورًا منه، كما ترتكب الجريمة إذا استمر الجاني بقائه داخل النظام بعد انتهاء الفترة المحددة لذلك بموجب الإذن أو التصريح[4]، وبناءً على الركن المادي تتميز جريمة البقاء غير المشروع بعدة سمات أبرزها: أنها جريمة شكلية[5]، وسلبية[6]، وجريمة مستمرة[7].

[1] مناصرة يوسف، المرجع السابق، ص 126-127.

[2] عزالدين عثماني، المرجع السابق، ص 617.

[3] بن مكي نجاة، المرجع السابق، ص 183.

[4] زينات طلعت شحادة، المرجع السابق، ص52- 53.

[5] أي من جرائم الخطر وليس جرائم الضرر، لأننا كثيراً ما نجد أن التشريعات التي تناولت هذه الجريمة اكتفت بالبقاء غير الشروع داخل نظام المعالجة الآلية للمعطيات من أجل إرساء التجريم دون النص على حصول نتيجة معينة. أنظر عمار عباس الحسيني، المرجع السابق، ص271.

[6] وتعتبر هذه جريمة امتناع بسبب احجام المستخدم عن الخروج من نظام المعالجة، على عكس جريمة الدخول غير المصرح به إلى نظام المعلومات التي تعتبر جريمة إيجابية لأن السلوك الاجرامي فيها يتمثل في فعل إيجابي وهو فعل الدخول، أنظر عمار عباس الحسيني، المرجع نفسه، 270- 271.

وتعتبر هذه جريمة امتناع بسبب احجام المستخدم عن الخروج من نظام المعالجة، على عكس جريمة الدخول غير المصرح به إلى نظام المعلومات التي تعتبر جريمة إيجابية لأن السلوك الاجرامي فيها يتمثل في فعل إيجابي وهو فعل الدخول

[7] لأن السلوك الاجرامي المكون للركن المادي يتطلب الاستمرار ولو كان سلوكا سلبيًا. أنظر عمار عباس الحسيني، المرجع نفسه، 271.

3_ الركن المعنوي:

إن جريمة البقاء غير المشروع هي جريمة عمدية مثلها مثل جريمة الدخول غير المشروع تتطلب توافر القصد الجنائي العام، فيعلم الجاني أنه بقي بعد دخوله في نظام المعالجة الآلية للمعطيات، وأن إرادته تتجه إلى البقاء في هذا النظام، ولا يهم الباعث الذي جعل الجاني يبقى على إتصال بنظام المعالجة الآلية للمعطيات الذي لا يحق له بالبقاء فيها[1]، فلا فرق إذا كان الباعث نبيل أو غير ذلك.

4- العقوبات:

نفس العقوبات المطبقة على الشخص الطبيعي والشخص المعنوي، في حالة جريمة الدخول غير المشروع.

فما يلاحظ على هذه الجرائم أن المشرع في جريمة الدخول غير المشروع وجريمة البقاء غير المشروع اعتمد على التجريم الوقائي والذي يعتبر من آليات التجديد في السياسة الجنائية المعاصرة، فهاتين الجريمتين تعتبران من جرائم الخطر وليس من جرائم الضرر كونهما إذا ارتكبتا يمكن أن تؤديان إلى عدة جرائم أخرى، لذا فالمشرع جرم جريمة فعل الدخول والبقاء وقاية من وقوع جرائم أخرى والتي ستفصل فيها في المقام الموالي.

[1] بن مكي نجاة، المرجع السابق، ص 184-185.

الفرع الثاني: الجرائم المرتبطة بجريمة الدخول أو البقاء غير المشروع

وهي تمثل الجريمة في صورتها المشددة أو جريمة الضرر، كما سبق وعرجنا أن المشرع الجزائري اكتفى في جريمة الدخول أو البقاء غير المشروع بمجرد حصول السلوك الإجرامي، دون النتيجة فاعتبارهما جريمتان شكليتان لا تتطلبان حدوث ضرر. لكن الإشكال يطرح هنا حول ما إذا نتجت نتيجة عن هذا الدخول أو البقاء غير المشروع جريمة؟ وفيما يتمثل الأثر القانوني المترتب على ذلك؟

إجابة على هذا السؤال المشرع حدد حصرًا نتائج معينة لتشديد الجريمة، وتتمثل في ثلاث نتائج مرتبة لهذا الاثر القانوني، وهي تخريب نظام المعالجة الآلية للمعطيات أو حذف أو تغيير معطياته، نصت المادة 394 مكرر من قانون العقوبات الجزائري في فقرتها الثانية والثالثة على هذا الأثر، والتي تقابلها المادة 323-1 من ق ع ف[1]، فهذا التشديد الغاية منه هي حماية النظام من خلال حماية معطياته من عملية الحذف أو التغيير، وحمايته هو في حد ذاته من التخريب الذي يؤدي إلى تعطيل قيامه بوظائفه، وعدم القدرة على تنفيذ المعالجة الآلية للمعطيات[2].

أولا: الجرائم الواقعة على معطيات نظام المعالجة الآلية

ما يلاحظ أن المشرع الجزائري في قانون العقوبات أضفى حماية على المعطيات بصفة عامة دون تحديد نوع هذا المعطيات (شخصية، حكومية ...)، وبالتالي هنا عندما ندرس الجرائم الواقعة على المعطيات فإن هذه الحماية الجنائية تتمثل في كل أنواع المعطيات.

[1] محمد خليفة، المرجع السابق، ص 160-161.

[2] غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، منشورات الدار الجزائرية، الجزائر، 2016، ص 169.

1_ جريمة تعديل أو حذف معطيات المنظومة نتيجة الدخول أو البقاء غير المشروع:

نصت عليها المادة 394 مكرر من قانون العقوبات الجزائري.

أ_ الركن المادي:

يتمثل السلوك في حذف أو تغيير معطيات النظام: فالحذف هو أي فعل يجعل المعطيات التي يحتويها نظام المعالجة الآلية غير موجودة أو غير متاحة لمستخدميه الشرعيين[1]، أما التغيير فهو استبدال المعطيات بمعطيات أو بمعلومات أو ببيانات أخرى عن طريق التلاعب بالبرامج وإظهار معطيات أو بيانات مغايرة عن تلك التي صمم بخصوصها البرنامج[2]، وما يجدر الإشارة إليه في هذا الصدد يرى الفقه أنه من الصعب أن يتم التمييز الفعلي بين فعل الحذف وفعل التغيير، لأنه غالبا عند القيام بفعل التغيير لابد من تنفيذ فعل الحذف[3]، وحتى يتم الأخذ بهذا التشديد لابد من وجود علاقة السببية بين سلوك الدخول أو البقاء غير المصرح به، والنتيجة الإجرامية الضارة والمتمثلة في محو أو تعديل المعطيات الموجودة في النظام[4].

[1] بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، مخبر الدراسات القانونية، جامعة ابن خلدون تيارت، الجزائر، المجلد 01، العدد 01، 2019، ص 82.

[2] بهاء المري، جرائم المحمول ووسائل التواصل الاجتماعي فيس بوك- انستجرام- واتس آب- تويتر - فايبر وحجية الدليل الالكتروني في الإثبات، ط 4، دار الأهرام للنشر والتوزيع والاصدارات القانونية، د. ب. ن، 2022، ص120-121.

[3] بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، المرجع نفسه، ص 82.

[4] غنية باطلي، المرجع السابق، ص 169.

ب_ الركن المعنوي:

جريمة تعديل أو حذف معطيات المنظومة نتيجة الدخول غير المشروع نصت عليها المادة 394 مكرر من قانون العقوبات الجزائري[1]، أما المادة 394 مكرر 1 من نفس القانون نصت على جريمة إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها والتي يطلق عليها جريمة الإعتداء العمدي على المعطيات أو جريمة التلاعب بالمعطيات[2].

من خلال مقارنة المصطلحات المستعملة في المادتين، نجد أن المصطلحات الواردة في جريمة تعديل أو حذف معطيات المنظومة نتيجة الدخول أو البقاء غير المشروع أي الصورة المشددة للجريمة لم يتم إستعمال مصطلح غش Fraudulesement، كما استعمل مصطلح حذف وتغيير ولم يستعمل مصطلح إدخال لأن هذا الفعل الأخير يكون عمدًا، هذا ما جعل جانب من الفقه يقول أن هذه الجريمة غير عمدية تكون خطأً حيث لا تتطلب قصد جنائي، ويكفي فيها الخطأ[3].

لأن الظروف المشددة هنا من الظروف المشددة المادية التي لا تغير من وصف (طبيعة) الجريمة والتي تقوم بمجرد قيام الركن المادي لها ومن خلال ترتب النتيجة المشددة وارتباطها بالفعل المجرم المتمثل في الدخول أو البقاء بعلاقة السببية[4].

---

[1] نصت المادة 394 مكرر من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، على أنه " ...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة..."

[2] نصت المادة 394 مكرر 1 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، على أنه "... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها ".

[3] بوكر رشيدة، الدخول أو البقاء داخل نظم معلومات المؤسسة الإقتصادية " بين عدم التصريح والحماية الجزائية"، مجلة قانون العمل والتشغيل، مخبر قانون العمل والتشغيل، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد 06، العدد 01، جانفي 2021، ص 214.

[4] محمد خليفة، المرجع السابق، ص 169.

وبالتالي لا يمكن تطبيق الظرف المشدد إذا قصد الجاني تحقيق النتيجة الإجرامية المتمثلة في تعديل أو حذف معطيات المنظومة نتيجة الدخول أو البقاء غير المشروع، **لأن** هذا الفعل يندرج ضمن المادة 394 مكرر1 من نفس القانون السابق الذكر وبالضبط يتمثل في جريمة الإعتداء العمدي على المعطيات أو جريمة التلاعب بالمعطيات[1].

ج_العقوبات:

إذا أدت جريمة الدخول أو البقاء عن طريق الغش في جزء أو كل من منظومة المعالجة الآلية للمعطيات إلى تغيير أو حذف لمعطياتها الرقمية، تضاعف العقوبة في هذه الجريمة[2]، حيث تصبح من (6) أشهر إلى سنتين (2) وبغرامة من 100.000 إلى 400.000 دج بالنسبة للشخص الطبيعي، وكذلك بالنسبة للشخص المعنوي فهي الغرامة المضاعفة خمس مرات عما هو مقرر للشخص الطبيعي[3].

ويمكن لجريمة الإعتداء العمدي على المعطيات أو جريمة التلاعب بالمعطيات أن تكون بشكل مستقلاً عن جريمة الدخول والبقاء غير المشروع كما سبق وذكرنا، والتي سنتطرق إليها على النحو التالي:

هذه الجريمة نصت عليها المادة 394 مكرر1 من القانون 04-15[4]، حيث يكون الاعتداء فيها على مستوى محتوى المعالجة يشتمل الركن المادي لهذه الجريمة على عنصر السلوك الاجرامي، وهذا الأخير يتكون من ثلاثة أفعال صور وهي الإدخال (L'introduction) والمحو(الإزالة) (L'effacement) والتعديل (Modification) [5]، فهذه

[1] بوكر رشيدة، المرجع السابق، ص 214

[2] أنظر المادة 394 مكرر من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[3] محمد خليفة، المرجع السابق، ص 174.

[4] نصت المادة 394 مكرر1 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات على أنه " يعاقب بالحبس من 6 أشهر إلى ثلاث 3 سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"

[5] غنية باطلي، المرجع السابق، ص 173.

الأفعال تغير الحالة التي توجد عليها معطيات النظام الواقع عليها الاعتداء، أي تؤدي إلى المساس بسلامتها والاخلال بها من ناحية تكاملها[1]، وعليه فإن المعطيات التي تمت معالجتها بواسطة نظام المعالجة الآلية للمعطيات تكون هي محل النشاط الإجرامي، أي المعطيات التي داخله، أو المدخلة فيه، والتي لم تتم إجراءات معالجتها، وبالتالي لا تقوم هذه الجريمة إذا وقع السلوك المجرم قبل أو بعد خروج المعطيات من نظام المعالجة الآلية ومثاله المعطيات المنصبة على الأقراص أو الأشرطة الممغنطة، ولا يشترط القانون اجتماعها، لكن يكفي أن يصدر من الجاني أحد هذه الأفعال، مع عدم وجود إذن أو تصريح بذلك، هذا ما يدل عنه مصطلح "بطريق الغش" الوارد في المادة السابقة الذكر[2].

ويقصد بفعل إدخال معطيات في نظام المعالجة الآلية إضافة معطيات جديدة غير موجودة من قبل على الدعامة الرقمية، ولا يهم إن كانت هذه الدعامة خالية أو محتواة على معطيات من قبل[3]، أما فعل التعديل فيقصد به تغيير المعطيات الموجودة داخل النظام أو إستبدالها بأخرى، ويتم هذا الفعل عن طريق برامج تتلاعب بالمعطيات[4]، أما فعل إزالة أو محو معطيات من نظام المعالجة الآلية فيقصد به إزالة كل أو جزء من المعطيات المحفوظة على الوسيط أو الدعامة الرقمية لنظام المعالجة الآلية للمعطيات أو إتلاف وتحطيم تلك الدعامة[5]، وعملية الإزالة والمحو تكون في المرحلة التي تلي عملية الإدخال[6]. وبخصوص النتيجة الإجرامية فتعتبر هذه الجريمة جريمة مادية من جرائم الضرر لا يكفي فيها تهديد

[1] محمد خليفة، المرجع السابق، ص179.

[2] غنية باطلي، المرجع السابق، ص 173- 174.

[3] علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة – دراسة مقارنة- ، ط 1، منشورات زين الحقوقية، 2013، ص 535./ بن مكي نجاة، المرجع السابق، ص188.

[4] غنية باطلي، المرجع نفسه، ص 176.

[5] أمحمدي بوزينة آمنة، خصوصية قواعد التجريم عن الإعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، مخبر الدراسات في الرقمنة وصناعة المعلومات الالكترونية بالمكتبات الأرشيف والتوثيق، جامعة العربي التبسي، تبسة، الجزائر، العدد 05، 2020، ص 81.

[6] بن مكي نجاة، المرجع السابق، ص188.

سلامة المعطيات وإنما لابد من انتهاك هذه السلامة وحدوث ضررًا فعليًا يتمثل في تغيير الحالة التي كانت متواجدة عليها المعطيات، والنتيجة في هذه الجريمة قد تتم بعد دخول أو بقاء مشروعين وتكون دائما عمدية يقصد الجاني إحداثها[1].

ويتوفر القصد الجنائي العام في هذه الجريمة حيث تتجه إرادة الجاني نحو هذه النتيجة، وتتجسد من خلال الأفعال الثلاثة المذكورة سابقا، وهو على علم بأن سلوكه مجرم وأنه يعتدي على صاحب المعطيات، وتتجه إرادته إلى مخالفة إرادة مالكها، أو من يسيطر عليها[2]. ولم يشترط المشرع الجزائري توافر **القصد الجنائي الخاص**[3] واكتفى فقط بالقصد العام[4].

العقوبات: بالنسبة للشخص الطبيعي العقوبة تتمثل في الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 4.000.000 دج. أما بالنسبة للشخص المعنوي فالعقوبة تعادل 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[5] أي تعادل 20.000.000 دج.

[1] محمد خليفة، المرجع السابق، ص 186- 187.

[2] بن مكي نجاة، المرجع السابق، ص 190.

[3] فالمادة 394 مكرر01 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات لا تتطلب توافر القصد الخاص، وإنما اكتفت بالقصد العام فقط، فالقصد الخاص هو انصراف الإرادة إلى وقائع لا تدخل ضمن عناصر الجريمة وأركانها، ولفظ الغش الوارد في المادة السالفة الذكر لا يدل على هذا المعنى، وإنما يدل على ضرورة توافر العمد، أي القصد الجنائي العام، وهو ما جاء في المادة 3/333 من قانون العقوبات الفرنسي، وتم تبرير الجمعية الوطنية الفرنسية إضافة مصطلح الغش لهذه المادة بأن إدخال المعطيات في نظام المعالجة الآلية للمعطيات وإزالتها أو تعديلها هي بالتحديد الوظيفة المخولة للمعلوماتيون ومستخدمو المعلوماتية، وبالتالي الجريمة لا تتحقق إلا إذا كانت هذه العمليات قد إرتكبت بقصد الغش وخارج الإستعمال المرخص به من طرف مقدمي الخدمات، وهناك من يرى أن مصطلح الغش في هذه المادة يعني وجود قصد خاص تتطلبه المادة السالفة وهو إرادة تسبيب ضرر للغير في ماله أو في حقوقه على إختلاف طبيعتها. أنظر محمد خليفة، المرجع نفسه، ص 187 – 189.

[4] باطلي غنية، المرجع السابق، ص 177.

[5] أنظر المادة 394 مكرر 5 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

وبالنسبة للشروع في ارتكاب هذه الجنحة تم النص عليه صراحة بموجب المادة 394 مكرر 7 من القانون رقم 04-15[1] حيث يُعاقب عليه بنفس العقوبة المقررة لهذه الجنحة[2]، وكذلك الأمر بالنسبة للمشاركة في مجموعة أو الاتفاق بغرض الشروع في جريمة[3]، أما بالنسبة للعقوبات التكميلية كذلك في هذه الجريمة يحكم بالمصادرة والغلق[4]- تم التفصيل فيها سابقا-

2_ جريمة التعامل في معطيات نظام المعالجة الآلية:

نصت المادة 394 مكرر2 على جريمة التعامل في معطيات نظام المعالجة الآلية، والتي تتخذ صورتين:

أ_ جريمة التعامل في معطيات صالحة لارتكاب جريمة:

يتمثل ركنها المادي في القيام عمدا وخلسة بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات تمكن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

فالنسبة للتصميم يقوم بهذه العملية متخصصي التصميم مثل مبرمجين ومصممي البرامج الحاسوبية، فهي تمثل المرحلة الأولى في سلسلة التعامل في المعطيات، من خلال إخراج المعطيات إلى الوجود، فالمختص في تصميم البرامج يقوم بإنشاء والعثور على معطيات صالحة لإرتكاب الجريمة، ومثالها تصميم برامج قرصنة، أو تصميم برامج ضارة تحمل فيروسات[5]، أما البحث فيتمثل في البحث في طريقة تصميم المعطيات وإعدادها وليس

[1] تنص المادة 31 من ق.ع.ج على أن "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا."

[2] أنظر المادة 394 مكرر 7 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[3] أنظر المادة 394 مكرر 5 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[4] أنظر المادة 394 مكرر 6 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[5] بن مكي نجاة، المرجع السابق، ص 194.

مجرد البحث عنها، لأنه في الأصل البحث عن الوسائل التي يمكن ارتكاب الجريمة بها لا يعتبر جريمة، أما التجميع فيعني القيام بجمع عدد كبير من المعطيات التي يمكن من خلالها ارتكاب جريمة الدخول غير المصرح به أو البقاء غير المشروع، أو جريمة التلاعب بالمعطيات، وبالنسبة للتوفير يكون من خلال توفير معطيات وإتاحتها لمن يريدها، وإتاحتها للآخرين ووضعها تحت تصرفهم[1].

أما فعل النشر يتمثل في إذاعة المعطيات والسماح للغير بالاطلاع عليها، من خلال الوسائل المختلفة للنشر[2]، وفعل الاتجار بالمعطيات يعني تقديم الشخص لمعطيات مقابل مبلغ مالي أو منفعة مادية أو معنوية[3].

وما يلاحظ على هذه المادة أنها جاءت ناقصة مقارنة بما يقابلها في التشريع المقارن، التي أضافت أفعالاً أخرى مثل الاستيراد، أو عرض، أو بيع، أي **معدات**[4] أو أدوات أو **برامج معلوماتية**[5] أو أي معطيات مصممة لارتكاب جريمة أو أكثر من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات هذا وفقا لقانون العقوبات الفرنسي[6]، والقانون المصري[7].

---

[1] قسمية محمد، خضري حمزة، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد 07، العدد 02، نوفمبر 2020، ص 140- 141.

[2] بن مكي نجاة، المرجع نفسه، ص 195.

[3] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 149.

[4] **جهاز أو المعدات** : أية أجهزة أو معدات أو مستلزمات تستعمل أو تكون معدة للاستعمال في خدمات الاتصالات مثل أجهزة استقبال الرسائل، كذلك الحاسب الآلي يعتبر من الأجهزة ومن المعدات أيضا التي تستعمل في شبكات الاتصال وفي شبكات المعلومات واعداد البيانات ونظم المعلومات، وأجهزة الهاتف المحمول، والكمبيوتر المحمول. محمد سيد عبد الوهاب أبو سريع وشهرتة محمد أبو الخير، المرجع السابق، 2022، ص259.

[5] **برامج معلوماتية:** تتمثل في الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفته أو تحقيق نتيجة، محمد سيد عبد الوهاب أبو سريع وشهرتة محمد أبو الخير، المرجع نفسه، ص 260.

[6] Art 323 -3-1,de la Loi n°88-19.

[7] المادة 22 من قانون مكافحة جرائم تقنيات المعلومات المصري.

ب_ جريمة التعامل في معطيات متحصلة من جريمة:

ويتمثل ركنها المادي في القيام عمدا وخلسة بحيازة أو إفشاء أو نشر أو إستعمال معطيات متحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فبنسبة لفعل الحيازة[1] يتمثل في السيطرة الفعلية على المعطيات الرقمية ذات الطبيعة المعنوية[2]، أما إفشاء أو نشر معطيات متحصل عليها يعني إذاعة المعطيات المتحصل عليها من طرف الجاني من دخوله غير المشروع لنظام المعالجة الآلية للمعطيات أو بقائه غير المشروع فيه[3]، وتعتبر هذه الجرائم من الجرائم الشكلية، فهي لا تتطلب حدوث نتيجة وإنما تقوم بمجرد ارتكاب السلوك الإجرامي.

وهذين الجريمتين عمديتين يتوفر فيهما العلم والارادة، وخلافا لما سبق استعمل المشرع مصطلح "**عمدًا**" إضافة إلى عبارة "**عن طريق الغش**" التي استعملها في الجرائم السالفة الذكر فقط لتأكيد القصد الجنائي العام، دون اشتراط قصد جنائي خاص[4].

وعقوبة جريمة التعامل في معطيات بصورتيها بالنسبة للشخص الطبيعي هي الحبس من شهرين(2) إلى ثلاث(3) سنوات وبغرامة من 500.000 دج إلى 10.000.0000دج، وبالنسبة للشخص المعنوي فعقوبته تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[5]، وعقوبة الشروع في ارتكاب هذه الجنحة نفسها العقوبة المقررة لارتكاب الجنحة في حد ذاتها[6]، ويعاقب بنفس العقوبة المقررة لهذه الجريمة في حالة الاشتراك والإتفاق لتحضير

[1] وكما نعلم أن للحيازة عنصران: عنصر مادي يتمثل في مجمل الأفعال التي تشكل الحيازة، وعنصر معنوي يتمثل في الظهور على الشيء كالمالك، للتفصيل أكثر أنظر رامي متولي القاضي، عمر سالم، المرجع السابق، ص 148.

[2] رامي متولي القاضي، عمر سالم، المرجع السابق، ص 148.

[3] بهاء المري، المرجع السابق، ص121.

[4] بن مكي نجاة، المرجع السابق، ص 200.

[5] أنظر المادة 394 مكرر6 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[6] أنظر المادة 394 مكرر7 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

لها، وتحقق هذا التحضير[1]، وفي هذه الجريمة يُحكم كذلك بالمصادرة، وغلق محل أو مكان الاستغلال إذا ما إرتُكبت الجريمة بعلم مالكها[2].

ثانيا: جريمة تخريب نظام تشغيل المنظومة على إثر الدخول أو البقاء غير المشروع

والمشرع الجزائري نص على جريمة تخريب نظام تشغيل المنظومة في م394 مكرر ق.ع كأثر مترتب عن الدخول أو البقاء غير المشروع، ولم ينص عليها بصور مستقلة[3]، والركن المادي يكون من خلال فعل إعاقة أو عرقلة النظام المعلوماتي وهي أفعال تمنع النظام المعلوماتي من أداء وظيفته بشكل صحيح، وعلى أكمل وجه، فيصبح مرتبكا، ويتوقف عن أداء وظيفته بشكل صحيح[4]، وكذلك فعل تعطيل أو توقيف النظام، والذي هو هو كل فعل يجعل نظام المعالجة الآلية للمعطيات عاجزًا أو مشلولًا سواء كان ذلك عن طريق فعل مادي يتم من خلال وسيلة مادية كالكسر أو التحطيم، أو معنوي يكون من خلال وسيلة معنوية كإدخال برنامج فيروس أو بتخزين فيه معطيات تتجاوز سعته الفعلية، من خلال استخدام تقنية التشبع "saturation " أو من خلال استخدام تقنية الفخ " trappe"، أو إستخدام التشويش"brouillage" أو بفعل الإفساد الذي يجعل نظام المعالجة الآلية يعطي نتائج غير مطابقة لتلك التي من الواجب الحصول عليها، ولا يتوجب أن يقع التعطيل أو الإفساد على

[1] أنظر المادة 394 مكرر5 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[2] أنظر المادة 394 مكرر6 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[3] وهذا خلافا للمشرع الفرنسي الذي نص على هذه الجريمة في صورتين، وهما جريمة تعطيل نظام المعالجة الآلية للمعطيات كجريمة مستقلة، والحالة الثانية جريمة تعطيل نظام المعالجة الآلية للمعطيات كنتيجة لارتكاب جريمة الدخول غير المشروع، وذلك في المادتين 2/323، ونص المادة 1/323 من قانون العقوبات الفرنسي الجديد ، وهذه الحالة الأخيرة هي التي يهمنا معالجتها، للتفصيل أكثر أنظر: محمد حماد مهرج الهيتي، المرجع السابق، ص 435.

[4] عمار عباس الحسيني، جريمة الإتلاف المعلوماتي- دراسة قانونية مقارنة-، ط 1، منشورات زين الحقوقية، بيروت لبنان، 2019، ص49.

جميع عناصر النظام المادية والمعنوية ، وأن تكون النتيجة توقف سير النظام كليا أو جزئيا بصورة دائمة أو مؤقتة[1].

وما يجدر الإشارة إليه هنا أن جريمة إتلاف النظام المعلوماتي تختلف عن جريمة إعاقة النظام المعلوماتي[2]، حيث في الأصل أن لكل من الجريمتين ذاتيتها المستقلة، لذا يفترض أنه من البديهي أن يكون لكل منهما نصوص قانونية خاصة وعقوبة مقررة لكل واحدة منهما، أو على الأقل تشديد عقوبة الإعاقة إن وصلت إلى إتلاف النظام كما جاء في قانون العقوبات الإيطالي، إلا أن هناك العديد من تشريعات تقرر العقوبة ذاتها لكل من الجريمتين[3]، ومن هذه التشريعات المشرع الجزائري الذي نص في م 394 مكرر ق.ع.ج.

وهذه الجريمة عمدية كما سبق وأن ذكرنا تتطلب القصد الجنائي بعنصريه العلم والإرادة.

أما بخصوص العقوبة المقررة لها هي الحبس من ستة أشهر إلى سنتين وغرامة من 50.000 دج إلى 300.000 دج هذا ما جاء في الفقرة الأخيرة من م 394 مكرر ق.ع[4]،

[1] زينات طلعت شحادة، المرجع السابق، ص 58- 59.

[2] الفرق بينهما: من حيث النتيجة الاجرامية: يمكن أن يؤدي هذا التخريب إلى إتلاف النظام المعلوماتي والمتمثل في التخريب أو تدمير أو 'التعطيل الكلي أو الجزئي لأنظمة المعلومات مما يؤدي إلى فقدان العناصر المنطقية المعطيات والبرامج والمعلومات والمحررات المعلوماتية، أما في جريمة الاعاقة التي تتطلب إرباك وعرقلة النظام المعلوماتي، ومن هنا يتضح لنا الفرق بين الإتلاف أو التدمير وعرقلة النظام، حيث الفرق يكمن في النتيجة الإجرامية فهي تقتصر في جريمة الإعاقة أو العرقلة على حدوث إرباك أو عرقلة لهذا النظام المعلوماتي لمنعه من أداء وظيفته بشكل صحيح، ومن هنا يتبين لنا أن إعاقة نظام المعالجة الآلية هي تعطيل مؤقت والإتلاف هو تعطيل دائم، ويظهر كذلك الفرق أيضًا من خلال القصد الإجرامي، حيث يهدف القصد الإجرامي لمرتكب إتلاف المعلومات إلى تقويض صلاحية العناصر المنطقية المذكورة سابقًا، وفقدان قدرتها على أداء الوظيفة المقصودة، وينطوي القصد الجنائي في جريمة إعاقة نظام المعلومات في عرقلته مؤقتًا أو إبطاء تشغيله، على الرغم من أن كلاهما يشكل جريمة عمدية ، يتوافر فيها القصد الجنائي بعنصريه العلم والإرادة، عمار عباس الحسيني، جريمة الإتلاف المعلوماتي – دراسة قانونية مقارنة–، المرجع نفسه، ص 60.

[3] عمار عباس الحسيني، جريمة الإتلاف المعلوماتي – دراسة قانونية مقارنة–، المرجع السابق، ص 60- 61.

[4] أنظر المادة 394 مكرر من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

ويعاقب الشخص المعنوي اذا ارتكب هذه الجريمة بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[1].

وما يجدر الإشارة إليه في هذا الصدد أن هذه الجريمة يمكن أن تكون في شكل جريمة ارهابية، من خلال إتلاف أو تدمير أنظمة الكمبيوتر الخاصة بالدول والشركات من خلال هجمات القراصنة[2].

وما يجب علينا الاشارة إليه في ختام هذا المطلب هو أنه إذا ارتكبت كل الجرائم السالفة الذكر في هذا المطلب أي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، إضرارًا بالدفاع الوطني تضاعف العقوبة وفقا لما نصت م394 مكرر3 من ق.ع.ج، وكذلك بما أن الجزائر كغيرها من الدول تبنت الحكومة الالكترونية[3]، وإستجابة لذلك تحولت من الإدارة الكلاسيكية نحو الإدارة الإلكترونية، فغالبية الهيئات والمؤسسات الخاضعة للقانون العام أصبحت إدارتها إلكترونية، وحماية لأنظمة المعالجة الآلية لهذه الهيئات والمؤسسات الخاضعة للقانون العام ولمعطياتها تم مضاعفة العقوبة إذا استهدفتها هذه الجرائم[4]. وما يجدر بنا الإشارة إليه في هذا الصدد أنه تم وضع منظومة وطنية لأمن الأنظمة المعلوماتية[5]، موضوعة لدى وزارة الدفاع الوطني التي تعتبر من الوزارات السيادية[6]، بغرض التصدي للتهديدات الالكترونية التي تستهدف المؤسسات الوطنية سواء كانت خاضعة

[1] أنظر المادة 394 مكرر4 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[2] G. Uricchio , Il Cyberterrorismo, in M. Iaselli (a cura di), Investigazioni digitali, Giuffrè Francis Lefebvre, Milano 2020, p 683.

[3] وضعت الجزائر برنامج خماسي 2009 – 2013 موسوم ب " الجزائر الالكترونية 2013".

[4] أنظر المادة 394 مكرر3 من القانون رقم 04-15 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات.

[5] أنظر المادة 1 من المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر.ج.ج ، العدد04، المؤرخة في أولى جمادى الثانية عام 1442ه الموافق 26 جانفي سنة 2020، ص6.

[6] حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي رقم 20-05، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 3، أكتوبر 2020، ص181.

للقانون العام أو القانون الخاص. وتم إستثناءًا أنظمة معلومات الدفاع الوطني من مجال تطبيق المرسوم الذي أوردها[1].

وتعتبر هذه المنظومة بمثابة إطار تنظيمي لإعداد استراتيجية أمن الأنظمة المعلوماتية الوطنية[2]. وتشتمل هذه المنظومة على المجلس الوطني لأمن الأنظمة المعلوماتية[3]، تتمثل مهمته الرئيسية في اعداد الاستراتيجية الوطنية لأمن أنظمة المعلوماتية، والموافقة عليها وتوجيهها[4]، ووكالة أمن الانظمة المعلوماتية[5]، وتتمثل مهمتها الرئيسية في تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية[6].

وما يلاحظ أن مجمل الجرائم التي أوردناها في هذا المطلب وردت في اتفاقية بودابست، فالمشرع الجزائري رغم عدم مصادقته على هذه الاتفاقية إلا أنه استحدثها في تشريعه العقابي لمكافحة هذه الجرائم المستحدثة، حتى لا يكون هناك فراغ تشريعي على المستوى وطني إذا ما تم إرتكاب جريمة من هذه الجرائم.

وحتى لا تكون ملقاة على عاتق الجزائر التزامات دولية، فإنها لم تصادق على هذه الاتفاقية، لأن هذه الاتفاقية أوربية النشأة في الأصل وبالتالي يغيب عنها التوجه العالمي البحت.

---

[1] أنظر المادة 40 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[2] أنظر المادة 2 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[3] يتكون من ممثل عن كل من رئاسة الجمهورية والوزير الأول، والوزير المكلف بما يلي: الشؤون الخارجية، الداخلية، العدل، المالية، الطاقة، الاتصالات، التعليم العالي. وللمجلس إمكانية الإستعانة بأي شخص أو مؤسسة لتنويره في أعماله. ويتم ترأس هذا المجلس من قِبل وزير الدفاع أو ممثله. أنظر أنظر المادة 5 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[4] أنظر المادة 3 من نفس المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[5] مقرها في مدينة الجزائر، هي مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية والستقلال المالي. أنظر المادة 17 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

[6] أنظر المادة 3 من المرسوم الرئاسي رقم 20-05 المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

المطلب الثاني: الجرائم الواقعة باستخدام أنظمة المعالجة الآلية للمعطيات

هناك نوع أخر من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وهي الجرائم التي ترتكب بواسطة النظام المعلوماتي أي التي يكون فيها النظام وسيلة لارتكاب الجريمة، وهذه الجرائم هي جرائم تقليدية لكن تكون فيها الوسيلة المستعملة حديثة، ومثالها: جرائم غسيل الأموا إلكترونيا، جرائم الإباحية الالكترونية، جرائم التجسس والتحريض ضد أمن الدولة الإلكترونية والجرائم الارهابية الالكترونية، فنظام المعالجة الآلية للمعطيات هنا ليس هدفا للجريمة، ولكن الحاسوب أو الهاتف الذكي وسيلة تُسهيل النتيجة الإجرامية باستخدام نظام المعالجة الآلية للمعطيات ويكون ذلك عبر منصات إلكترونية، والغرض الرئيسي منها هو الكسب بشكل غير مشروع، والإعتداء على الأموال، والتعدي على خصوصيات الأشخاص والاعتداء على أمن الدولة[1].

الفرع الأول: جرائم مواقع التواصل الإجتماعي

تساهم مواقع التواصل الاجتماعي، نظرًا لاستيعابها للبيانات والمعطيات الضخمة، في إمكانية نشر أي موضوع دون قيود، لذا تزيد إحتمالات إستخدام هذه المواقع بطريقة غير مشروعة، ووفقا لهذا يتزايد الخطر ما دامت هذه التجاوزات تؤدي إلى زعزعة أمن واستقرار المجتمع من خلال بث الفوضى والكراهية بين المواطنين، وإثارة الصراعات والفتن بين جميع الطوائف عن طرق الإنترنت[2]، ومرد تفاقم هذه الجرائم عدة أسباب أهمها خاصية هذه المواقع التي تمكن الأفراد من الولوج لها دون فرض أي قيود أو رقابة، فتمس حريتهم في التعبير،

[1] سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، المركز الديمقراطي العربي، مجلة العلوم السياسية والقانون، العدد 1، 2017، ص 271.

[2] مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام (دراسة تحليلية)، قدمت هذه الرسالة إستكمالا لمتطلبات الحصول على درجة الماجيستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الأزهر غزة، فلسطين، 1439هـ- 2017، ص74.

وكذلك غياب إقرار للمسؤولية الجزائية، وتداول المعلومات فيها يكون سريعا ومنتشرا وغير محدود، وساهمت في هذا كذلك الحسابات الشخصية الوهمية ومواقع الويب المزيفة[1].

أولا: مفهوم مواقع التواصل الاجتماعي

حتى يتضح لنا مفهوم مواقع التواصل الاجتماعي لابد من تعريفها:

1_ تعريف مواقع التواصل الإجتماعي:

يعرفها زاهر راضي "منظومة من الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثم ربطه عن طريق نظام إجتماعي إلكتروني مع أعضاء آخرين لديهم الإهتمامات والهوايات نفسها"[2]، وتعرف كذلك بأنها " شبكات اجتماعية تفاعلية تتيح التواصل لمستخدميها في أي وقت وفي أي مكان في العالم، ظهرت على شبكة الانترنت منذ سنوات وتمكنهم من التواصل المرئي والصوتي وتبادل الصور وغيرها من الامكانات التي توطد العلاقات الاجتماعية بينهم"[3].

[1] فاطمة الوحش، لهذه الأسباب انتشر خطاب الكراهية عبر مواقع التواصل، مقال منشور على الرابط التالي:
http://www.ech-chaab.com/ar/%D8%A3%D8%B9%D9%85%D8%AF%D8%A9-%D9%88-%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%AD%D9%88%D8%A7%D8%B1%D8%A7%D8%AA/item/186619-%D9%84%D9%87%D8%B0%D9%87-
تم الاطلاع عليه بتاريخ 2023/07/06 على الساعة 10:15.

[2] نبيل لحمر، الأخبار الكاذبة عبر شبكات التواصل الاجتماعي وآثارها على اتجاهات الرأي العام دراسة في المفهوم، العلاقة والأهداف، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة 11 الحاج لخضر، باتنة، الجزائر، المجلد 07، العدد02، جوان 2020، ص585. تم الاطلاع عليه بتاريخ 2023/07/06

[3] دنيا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الاسكندرية، مصر، المجلد 2، العدد 2، يوليو 2019، ص 225-226.

2 _ أنواع مواقع التواصل الإجتماعي:

أ_ موقع فيس بوك (FACEBOOK) : بدأت بالظهور مواقع التواصل الإجتماعي سنة 2004[1]، وارتفعت أعدادها بعد ذلك، وأشهرها موقع فيس بوك، حيث يعتبر الأكثرها إنتشارًا وإستخدامًا في العالم[2]، وفي الجزائر يعتبر أكثر المواقع استخداما بمعدل ارتفاع يصل إلى 1.5 مليون مشترك كل سنة[3]، وما يجدر الاشارة اليه أن هذا الموقع تفرعت منه الكثير من التطبيقات الأخرى مثل الماسنجر، والانستجرام وكذلك تطبيق الواتس آب، والفايبر.

ب_ موقع تويتر(TWITTER): كما ظهر موقع تويتر في عام 2006، يوفر خدمة التدوينات المصغرة، والرسائل النصية، يتيح لمستخدميه بنشر تدوينات بحد أقصى 280 حرفًا للرسالة الواحدة، والتي تعرف بالتغريدات[4].

ج_ موقع يوتيوب (YouTube): وهو أحد أشهر المواقع العالمية المجانية، يتيح لمستخدميه مشاهدة تسجيلات مرئية أو صوتية مجانا وكذلك الاستماع إليها ومشاركتها مع الجمهور، والتعليق عليها. ويطبق هذا الموقع سياسة هامة حيث يحظر مشاركة الأفلام إباحية، ولا إعلام مناهض[5].

---

[1] حيث في البداية تم إطلاق هذا الموقع في سنة 2004 من طرف مارك زوكربيرج لطلبة جامعة هارفورد Harvard فقط، ثم امتد إلى بقية الجامعات ليصل عدد مشتركيه في ديسمبر 2004 حوالي مليون مشترك، وفي الشهر التاسع من سنة 2006 أصبح هذا الموقع مفتوح لكل مستخدمي الانترنت في العالم. بلخير محمد آيت عودية، الضبط الإداري للشبكات الإجتماعية الإلكترونية، أطروحة مقدمة لنيل دكتوراه علوم في الحقوق، تخصص قانون عام، جامعة باتنة 1، كلية الحقوق والعلوم السياسية، 2019/2018، ص37.

[2] بهاء المري، المرجع السابق، ص39.

[3] بلخير محمد آيت عودية، الضبط الإداري للشبكات الإجتماعية الإلكترونية، المرجع نفسه، ص37.

[4] بهاء المري، المرجع نفسه، ص39.

[5] بهاء المري، المرجع السابق، ص39.

د_ إنستجرام (Instagram): ظهر سنة 2010 وخدمة لمشاركة الصور، ويتيح للمستخدمين التعارف ومتابعة الأشخاص المختلفين سواء ممن يعرفهم أو لا يعرفهم[1]، وهو الأخر موقع مجاني لتبادل الصور والفيديوهات، ويتيح لمن يستخدمه بمشاركتها ونشرها، وهو أحد تطبيقات التواصل الاجتماعي التي تكون في الهواتف المحمولة الذكية أيضا، ويمكن للشخص عرض أخباره عليه مثله مثل موقع الفايسبوك والتويتر[2].

هـ_ تطبيق" واتس آب" (whatsapp) وتطبيق الفايبر (viber): كلاهما يعتبر من وسائل التواصل الاجتماعي المجانية[3]، يتيح خدمة تبادل الرسائل النصية والصور ومقاطع الفيديو للتواصل فيما بين الأفراد، ويوفر المراسلة الفورية بين مستخدميه[4].

ثانيا: أشكال جرائم مواقع التواصل الإجتماعي

كذلك تنوعت الجرائم المرتكبة عبر مواقع التواصل الإجتماعي وانقسمت إلى عدت أنواع هي الأخرى:

1_ جرائم الأشخاص عبر مواقع التواصل الإجتماعي:

أتاحت الثورة الرقمية من خلال استخدام وسائل التواصل الاجتماعي تحقق أغلب صور الاعتداء على الأشخاص[5]، وتتمثل في:

[1] أسامة حسين محي الدين عبد العال، تجريم الشائعات عبر وسائل التواصل الاجتماعي في التشريع الجنائي المصري دراسة تحليلية، مجلة العلوم الإقتصادية والقانونية، كلية الحقوق، جامعة عين الشمس، مصر، العدد 1، السنة 63، يناير "الجزء 1" 2021، ص12.

[2] بهاء المري، المرجع نفسه، ص39.

[3] إكرام سليمان قجم، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، رسالة قُدمت استكمالا لمتطلبات كلية القانون للحصول على درجة الماجستير في القانون الخاص، جامعة قطر، كلية القانون، يونيو 2021، ص23.

[4] بهاء المري، المرجع نفسه، ص39- 40.

[5] علي جعفر، المرجع السابق، ص 173.

أ_ جرائم الإعتداء على الحياة الخاصة عبر وسائل التواصل الاجتماعي:

تعد مواقع التواصل الاجتماعي مستودعًا لأسرار المستخدمين ومعلوماتم وخصوصيتهم، فجميع هذه المواقع وعلى سبيل المثال فيس بوك (Facebook) يستخدم بيان الخصوصية أو سياسة الخصوصية، وهذه السياسة تختلف من موقع إلى أخر، وتجدر الاشارة إلى أنه هذه الشركة قد تستخدم معلومات وتبيعها لشركات أخرى، وحتى عند إلغاء الحساب فإنه لا يُلغى نهائيا بل يُعطل ويتم الاحتفاظ بالصور ومختلف المعلومات الأخرى التي يتضمنها، فعلى الرغم من وجود إعدادات الخصوصية إلا أنها لا تحمي المستخدم إلا من بقية الأعضاء الموجودين في الشبكة، ولكنها لا تمنع ظهور بياناته الشخصية للمالكين، وعليه فجميع المعلومات الشخصية والبيانات من صور ومقاطع الفيديو التي ينزلها الشخص على موقعه تهددها مخاطر الخصوصية نتيجة لسجلات الخوادم التي تسجل جميع أرقام "IP" للمستخدمين الذين يقومون بالاتصال بالخوادم[1].

ب_ جريمة السب والقذف عبر مواقع التواصل الاجتماعي:

نصت المادة 296 من ق.ع.ج على أن القذف يتمثل في كل واقعة من شأنها المساس بشرف واعتبار الأشخاص، حتى ولو تم ذلك دون ذكر اسم الشخص أو الهيئة، ولكن كان من الممكن تحديده، وورد فيها كذلك أنه يعاقب على نشر هذا الإدعاء مباشرة أو بطريقة إعادة النشر[2]، وما يلاحظ أن المشرع الجزائري لم يحدد طريقة النشر ما إذا كانت إلكترونية

[1] علي نعمة جواد الزرفي، المرجع السابق، ص51.

[2] المادة 296 من القانون رقم 06- 23 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006، يعدل ويتمم الأمر 66- 156 المتضمن قانون العقوبات، ج.ر.ج.ج، العدد84، المؤرخة في 4 ذي الحجة عام 1427 هـ، الموافق 24 ديسمبر سنة 2006 تنص على أنه: " يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو اسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة."

أم لا أو عبر مواقع التواصل الاجتماعي أم المواقع الالكترونية، وعليه من المستحسن أن يحدد المشرع الجزائري طريقة النشر وإعادة النشر تحديدا دقيقا، وفقا لما يقتضيه مبدأ الشرعية، ويضيف عبارة "**النشر أو إعادة النشر بأي وسيلة كانت**" لأن هذه الجريمة انتشرت في الآونة الأخيرة بشكل كبير.

وحسنا فعل المشرع عند معاقبته على إعادة النشر واعتبره سلوك مجرم حتى لا تنتشر جريمة القذف بصورة أكبر.

2_ جرائم الأموال عبر مواقع التواصل الإجتماعي:

تنقسم جرائم الأموال التقليدية بشكل عام، إلى جرائم السرقة، والنصب، والاحتيال، وخيانة الأمانة، إلا أنه بظهور مواقع التواصل الإجتماعي اتخذت هذه الجرائم محلا جديدا يتمثل في هذه البيئة الافتراضية للشبكات الاجتماعية، ومن أبرزها جريمة النصب والاحتيال عبر مواقع التواصل الاجتماعي فهذه الجريمة المستحدثة لا تختلف في فحوها عن جريمة الاحتيال التقليدية، فكلهما يستعمل الجاني وسائل احتيالية لأجل الاستيلاء على أموال الأخرين، بينما يكمن الاختلاف في محل السلوك الإجرامي من جهة وفي نوع الوسائل والأساليب الاحتيالية التي يستخدمها الجاني من جهة أخرى[1]، حيث هذه الجريمة المستحدثة ترتكب بواسطة مواقع التواصل الإجتماعي بمختلف أنواعها، يقوم المجرم المعلوماتي بعرض إمتيازات أو خدمات وسلع وهمية والإيحاء بالحصول على أموال، ما يجر ضحاياهم تدريجيا وفقًا لخطوات إحتيالية، وشهدت جرائم النصب والاحتيال عبر هذه المواقع ارتفاعا كبير في الجزائر، ولاسيما في فترة جائحة كوفيد وبالضبط في سنة 2020، حيث تم تسجيل ومعالجة 152 قضية نصب والإحتيال عبر الإنترنت، ووقِف 216 مشتبه فيه، وذلك ابتداء من تاريخ

[1] سامر سلمان الجبوري، جريمة الاحتيال الالكتروني دراسة مقارنة، ط 1، مكتبة زين الحقوقية والأدبية، بيروت، لبنان، 2018، ص 17.

الفاتح من جانفي 2020 إلى غاية 30 سبتمبر 2020[1]، ونظرا لإنتشار هذه الجريمة الهائل والتخوف من تفاقمها أكثر تم انتهاج طرق لتوعية والتحسيس بخصوصها[2]، لغرض التقليل منها.

3_ الجرائم الماسة بأمن الدولة عبر مواقع التواصل الإجتماعي:

تعتبر جريمة التحريض على الجرائم الإرهابية والنيل من الوحدة الوطنية على مواقع التواصل الاجتماعي، من أبرز الأمثلة للجرائم الماسة بأمن الدولة عبر مواقع التواصل الاجتماعي:

_ التدبير للأفعال الارهابية أو الإعداد لها أو المشاركة فيها أو التدريب على إرتكابها وكذلك جمع الأموال بأي وسيلة فلم يحدد المشرع هنا الوسيلة المستعملة وبالتالي يمكن أن تكون من

[1] الموقع الرسمي للمديرية العامة للأمن الوطني، متوفر على الرابط التالي:
https://www.algeriepolice.dz/?%D8%A7%D9%84%D9%85%D8%AF%D9%8A%D8%B1%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A-%D8%AA%D8%B9%D8%A7%D9%84%D8%AC-152-%D9%82%D8%B6%D9%8A%D8%A9,15007

تم الإطلاع عليه بتاريخ: 2023/05/01 على الساعة: 11:04.

[2] أطلقت المديرية العامة للأمن الوطني من خلال صفحتها الرسمية على الفايسبوك والتويتر، حملة توعية حول جرائم النصب والإحتيال عبر الأنترنت، دعت مستخدمي شبكات التواصل الإجتماعي والأنترنت لاسيما الأولياء، إلى أخذ الحيطة واليقظة والحذر من حيل الهاكرز والمحتالين، اللذين يستخدمون الرسائل الكاذبة التي تتيح لهم الحصول على المعطيات الشخصية وكلمات المرور المرتبطة بحسابات ضحاياهم أو سرقة هويتهم الرقمية، كما يدعو إلى مراقبة الأطفال عند استخدامهم الانترنت وتعريفهم بعيوبه. الموقع الرسمي للمديرية العامة للأمن الوطني، متوفر على الرابط التالي:

https://www.algeriepolice.dz/?%D8%A7%D9%84%D9%85%D8%AF%D9%8A%D8%B1%D9%8A%D8%A9-%D8%A7%D9%84%D8%B9%D8%A7%D9%85%D8%A9-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A-%D8%AA%D8%B9%D8%A7%D9%84%D8%AC-152-%D9%82%D8%B6%D9%8A%D8%A9,15007

تم الإطلاع عليه بتاريخ: 2023/05/01 على الساعة: 11:04.

خلال مواقع التواصل الاجتماعي بقصد استخدامها في تمويل سفر أشخاص إلى دولة أخرى، وهذا باستخدام تكنولوجيات الإعلام والاتصال[1].

_ كذلك جريمة نشر الأفكار الارهابية عبر مواقع التواصل الاجتماعي وتجنيد الأشخاص من خلالها ودعم أعمالها وأنشتطتها[2]، حيث يتم التجنيد من خلال مواقع التواصل الإجتماعي، فتمر العملية بعدة مراحل، بداية من نشر معلومات وأفكار بين الجماعة الإرهابية المتطرفة، ثم نشر الأفكار التي تتم من خلالها الدعاية، والمتمثلة مثلا في تعظيم الرغبة في الاستشهاد باعتباره طريقا للجنة، ثم تتم عملية الإستقطاب عبر هذه المواقع، سواء عن طريق وسطاء، أو إرسال الشخص بنفسه رسالة إلى هذه الجماعات أو يتم دعوته من طرف صديق للإنضمام إلى تلك المجموعات، ثم يتم تشكيل خلية التجنيد، ثم في المرحلة التالية لهذه المرحلة يتم تأصيل الأفكار التكفيرية والمتطرفة في أذهان الفئة المستهدفة والتي في الغالب

[1] المادة 87 مكرر 11 من القانون رقم 16- 02 المؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو 2016 المعدل والمتمم لقانون العقوبات، ج.ر.ج.ج، العدد37، مؤرخة في17 رمضان عام 1437 الموافق 22 يونيو 2016، تنص على أنه: " يعاقب بالسجن المؤقت من خمس (5) إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل جزائري أو أجنبي مقيم بالجزائر، بطريقة شرعية أو غير شرعية، يسافر أو يحاول السفر إلى دولة أخرى بغرض ارتكاب أفعال إرهابية أو تدبيرها أو الإعداد لها أو المشاركة فيها أو التدريب على ارتكابها أو لتلقي تدريب عليها.

يعاقب بنفس العقوبة كل من:

- يوفر أو يجمع عمدا موالا بأي وسيلة وبصورة مباشرة أو غير مباشرة، بقصد استخدامها أو مع علمه بأنها ستستخدم في تمويل سفر أشخاص إلى دولة أخرى بغرض إرتكاب الأفعال المذكورة في الفقرة الأولى من هذه المادة،
- قام عمدا بتمويل أو تتأو لقلقي تدريب عليها أو تسهيل ذلك السفر،
- يستخدم تكنولوجيات الإعلام والاتصال لارتكاب الأفعال المذكورة في المادة."

[2] المادة 87 مكرر 11 من القانون رقم 16- 02 المعدل والمتمم لقانون العقوبات تنص على أنه: " يعاقب بالسجن المؤقت من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها أو ينشر أفكارها بصورة مباشرة أو غير مباشرة".

تتمثل في الشباب وذلك من خلال الخطب الصوتية والأناشيد على اليوتيوب، ثم يتم تنويمهم مغناطيسيا، ثم تتم باقي عملية التغذية الفكرية وتليها مرحلة التنفيذ[1].

الفرع الثاني: نماذج مستحدثة للجرائم المرتكبة عبر مواقع التواصل الاجتماعي

في الآونة الأخيرة إستفحلت عدة جرائم تُرتكب عبر مواقع التواصل الاجتماعي، أصبحت مواقع التواصل الاجتماعي منصات خصبة لجرائم لخطابات الكراهية وجرائم التمييز والتحريض على التمييز والكراهية، ونشر الأخبار الكاذبة والمغلوطة، وفي هذا الفرع سنتطرق إلى هذين النموذجين من الجرائم المستحدثة المرتكبة عبر مواقع التواصل الإجتماعي، وهي جرائم التمييز وخطاب الكراهية في مواقع التواصل الإجتماعي (أولا)، جريمة نشر وترويج أخبار كاذبة أو مغرضة في مواقع التواصل الإجتماعي (ثانيا).

أولا: جرائم التمييز وخطاب الكراهية في مواقع التواصل الإجتماعي

نظرا للوضع الذي شهدته الجزائر أثناء الحراك الشعبي تفاقمت ظاهرة التمييز وانتشر خطاب الكراهية على مواقع التواصل الاجتماعي، وظهرت خطابات تحمل في طياتها ما يشتمل على التمييز والكراهية واستعملت فيها عبارات تمس بالوحدة الوطنية والهوية العربية والامازيغية وغابت خطابات التسامح والأخوة. ولخطورة هذه الظاهرة، ولمساسها بالصكوك الدولية، تمت دسترة خطابات الكراهية والتمييز في التعديل الدستوري الجزائري لسنة 2020

[1] شريفة كلاع، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، مركز المدار المعرفي للأبحاث والدراسات، الجزائر، المجلد 2، العدد السادس، سبتمر 2018، ص 87-89.

بموجب ديباجة هذا الدستور[1]، وفي نفس السنة تم إرساء قانون مستقل للوقاية منها ومكافحتها، يتمثل في قانون الوقاية من التمييز وخطاب الكراهية ومكافحتهما[2].

1 _ مفهوم جرائم التمييز والكراهية:

عرفته المادة الأولى من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية، خطاب الكراهية بأنه مختلف أشكال التعبير التي تنشر التمييز أو تشجعه أو تبرره، وكذلك جميع أشكال التعبير المتضمنة للإزدراء أو الإهانة أو العداء أو البغض أو العنف، والتي تكون موجهة إلى شخص أو مجموعة من الأشخاص على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الإثني أو اللغة أو الإنتماء الجغرافي أو الإعاقة أو الحالة الصحية.

أما التمييز فهو كل تفرقة أو إستثناء أو تقييد أو تفضيل تكون على أساس العرق أو اللون أو النسب أو الأصل القومي أو الإثني أو اللغة أو الإنتماء الجغرافي أو الإعاقة أو الحالة الصحية، يكون بهدف أو تعطيل أو عرقلة الإعتراف بحقوق الإنسان وحرياته الأساسية أو التمتع بها أو ممارستها على قدم المساواة، وذلك في مختلف المجالات السياسية أو الإقتصادية أو الإجتماعية أو الثقافية أو في أي مجال من مجالات الحياة العامة[3].

وعرف الفقه خطاب الكراهية بأنه " خطاب الكراهية هو نوع من الأحاديث التي تتضمن هجوما أو تحريضا أو انتقاصًا من فرد واحد أو عدة أفراد بناءا على عرقهم أو دينهم أو نوعهم الاجتماعي أو آرائهم السياسية أو الطبقة الاجتماعية التي ينتمون إليها، ودائما ما

---

[1] تمت إضافة العبارة التالية:" إن الشعب عازم على جعل الجزائر في منأى عن الفتنة والعنف وعن كل تطرف، **وعن خطابات الكراهية وكل أشكال التمييز**...." في دستور سنة 2020، والتي لم تكن واردة في ديباجة دستور 2016.

[2] القانون 20-05 المؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما. ج.ر.ج.ج، العدد 25، المؤرخة في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020.

[3] أنظر: المادة الاولى من القانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

يكون خطاب الكراهية أداة محفزة ومثيرة للمشاعر ومعبئة لها في اتجاه معين، فيصبح هذا الخطاب خطابا تحريضيًا وحاشدًا ينتج عنه سلوكا تمييزيًا وثقافة العنصرية وانتقاص حقوق الأفراد الذين يوجه ضدهم هذا الخطاب"[1].

يقصد بجرائم الكراهية كل سلوك إجرامي متعمد يكون ضد الأشخاص أو ممتلكاتهم، بسبب انتمائهم الحقيقي أو المفترض لفئة إجتماعية محددة، حيث يستهدف الجاني ضحيته بسبب دينهم أو معتقداتهم أو اللون أو العرق أو الأصل القومي، والذي يميز هذه الجريمة عن غيرها من الجرائم المشابهة التي تختلط بها هي الكراهية لفئة إجتماعية معينة، أو التعصب وعدم التسامح تجاه هذه الفئة[2].

2_ أركان جرائم التمييز والكراهية عبر مواقع التواصل الاجتماعي:

نصت على هذه الجريمة المادة 34 من القانون رقم 20-05[3]، ويتمثل السلوك الإجرامي في جريمة التمييز وخطاب الكراهية في سلوك إيجابي، ويتكون من عدة عناصر:

_ إنشاء أو إدارة أو الإشراف على **موقع إلكتروني** يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع

[1] مرو رياض علي أبو ظريس، مراد عبد الله المواجدة، أشكال خطاب الكراهية على مواقع التواصل الاجتماعي في المجتمع الأردني من وجهة نظر العاملين في وحدة مكافحة الجرائم الالكترونية، مجلة التربية، جامعة الأزهر كلية التربية بالقاهرة، مصر، العدد 189، الجزء الخامس، يناير 2021، ص449.

[2] منال مروان منجد، جرائم الكراهية: دراسة تحليلية مقارنة، مجلة جامعة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد 15، العدد1، يونيو 2018، ص174.

[3] المادة 34 من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما تنص على أنه "دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشرة (10) سنوات وبغرامة من 5.000.000 دج إلى 10.000.000 دج كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع".

_ إنشاء أو إدارة أو الإشراف على **حساب إلكتروني** يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع:

والموقع الالكتروني لم يعرفه المشرع الجزائري وهذا خلافا للمشرع المصري الذي عرفه في قانون مكافحة جرائم تقنية المعلومات بأنه: " مجال أو مكان إفتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة"[1]. فالموقع الالكتروني يقوم بتوفير المعلومات الإلكترونية على شبكة المعلومات، بما في ذلك مواقع التواصل الاجتماعي والصفحات الشخصية والمدونات[2].

عادةً ما يكون موقع الويب مملوكًا لشخص أو منظمة وهو مخصص لموضوع أو أكثر من الموضوعات، ومن خلالها الموقع يمكن لأصحابها نشر أي مادة يرغبون فيها[3]، بما في ذلك الأفكار والصور والرسومات والمعلومات التي تضفي طابع التمييز والكراهية.

والحساب الالكتروني لم يعرفه كذلك المشرع الجزائري، لكن تم تعريفها في التشريعات المقارنة والتي مثالها المشرع المصري الذي عرفه بأنه "مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له دون غيره الحق في الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي"، والحسابات الخاصة أشهرها صفحات التواصل الاجتماعي على شبكات التواصل الاجتماعي وهي مجموعة من المواقع على الانترنت ينشئها أفراد أو مؤسسات تتيح التواصل غير المباشر بين الأشخاص[4]، وفعل الإنشاء هو الاصطناع من العدم أي إنشاء موقع إلكتروني أو حساب إلكتروني لم يكن

[1] المادة 2 من قانون رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر (ج)، الصادرة بتاريخ 14 أغسطس سنة 2018.

[2] أنظر المادة 01 من القانون الاتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

[3] بهاء المري، المرجع السابق، ص128.

[4] بهاء المري، المرجع نفسه، ص 152.

موجودا من قبل[1]، أما فعل الإدارة أو الإشراف على موقع إلكتروني أو حساب إلكتروني يكون من خلال التحكم فيه والتسيير له، واستخدام الجاني للحساب أو الموقع في لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع، وتعتبر جرائم التمييز والكراهية جرائم عمدية تتطلب وجود العلم والإرادة.

3_ العقوبات المقررة لجرائم التمييز والكراهية عبر مواقع التواصل الاجتماعي:

بالنسبة للشخص الطبيعي يُعاقب على جريمة التمييز وخطاب الكراهية باستخدام تكنولوجيات الإعلام والإتصال بالحبس من سنتين إلى 5 سنوات وبغرامة من 200.000 دج إلى 500,000 دج[2]، ويعاقب بالحبس من خمس (5) سنوات إلى عشرة (10) سنوات وبغرامة من 5.000.000 دج إلى 10.000.000 دج كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب إلكتروني يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع[3].

وبالنسبة للشخص المعنوي يعاقب بالعقوبة المقررة في قانون العقوبات هذا وفقا للمادة 38 من القانون 20-05، وذلك بالرجوع إلى الباب الأول مكرر من قانون العقوبات المعنون ب " العقوبات المطبقة على الأشخاص المعنوية".

أما عقوبة الشروع على هذه الجنحة بنفس العقوبات المقررة في حالة ارتكاب الجنحة في حد ذاتها[4].

[1] محمد سيد عبد الوهاب أبو سريع وشهرته، محمد أبو الخير، المرجع السابق، ص287.

[2] أنظر المادة 31 من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

[3] أنظر المادة 34 من القانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

[4] أنظر المادة 39 من القانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

4_ أشكال خطاب التمييز والكراهية عبر مواقع التواصل الاجتماعي:

قد يتخذ خطاب الكراهية والتمييز عبر مواقع التواصل الاجتماعي عدة أشكال منها خطاب التمييز والعنصرية وهو أي خطاب يقوم على أساس التمييز أو العنصرية على أساس الانتماء الديني، أو السياسي أو الفكري أو الجنس أو العرق، وقد يتخذ شكل خطاب التحريض على التمييز والكراهية وهو كل خطاب يشجع على القيام بهذه الجريمة، وقد يكون خطاب يحمل الاستهزاء والسخرية والازدراء والاهانة على الانتماء الجغرافي والحالة الصحية، وكذلك قد يتخذ شكل خطاب التنافر الفكري والذي يعتبر من أبرز أشكال الكراهية، لأن شبكة الانترنت أتاحت لأصحاب الفكر المتعصب والمتطرف وبأسماء وهمية على مواقع التواصل الاجتماعي عملية التواصل والاتصال بينهم، ونشر الخطابات التي تحرض على التفرقة بمختلف أنواعها: عرقية، دينية، وأصبحت هذه الخطابات مصدرا منشأ للجريمة والعنف التي أصبح يعبر عنها اليوم ب "الحرائق الرقمية" [1].

ثانيا: جريمة نشر وترويج أخبار كاذبة أو مغرضة في مواقع التواصل الإجتماعي

لكل فرد الحق في تداول المعلومات بأي وسيلة كانت، وهذا حق تضمن ممارسته العديد من القوانين على المستوى الدولي والوطني[2]، لكن هذا الحق ليس مطلقًا كونه يصطدم بأفعال تشكل جريمة نشر وترويج أخبار كاذبة أو مغرضة في مواقع التواصل الاجتماعي إذا ما تم تغيير الحقيقة وتحريفها، ويطلق عليها كذلك تسمية جريمة الشائعة، نصت عليها العديد من التشريعات ومنها المشرع الجزائري الذي استحدثها بموجب القانون رقم 20-06 المؤرخ في 2020/04/28 الفصل السادس مكرر والذي جاء معنون ب "نشر وترويج أخبار

[1] فريد صحراوي، مكافحة خطاب الكراهية في البيئة الرقمية دراسة على ضوء القانون 20-05، دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر، المجلد 06، العدد 01، 2022، ص10

[2] نزيه محمد على عبد الغني، تداول المعلومات في الحد من آثار الشائعات على ضوء التشريعات الدولية والوطنية، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين الشمس، مصر، العدد 1، السنة 63، يناير 2021، ص 535.

أو أنباء تمس بالنظام العام والأمن العموميين، والذي تضمن مادة واحدة تجرم نشر الأخبار الكاذبة، وهذه المادة جرمة نشر وترويج الأخبار الكاذبة على كل الأشخاص ولم تقتصر على الأشخاص المختصة بنشر الأخبار كالصحفيين.

1_ ظروف استحداث النص الذي يجرم نشر الأخبار الكاذبة والمغرضة في قانون العقوبات الجزائري:

كما نعلم أن القانون وليد بيئته، فدائما يكون التجريم لاحق لارتكاب الواقعة المادية، فعندما ظهر وباء " كوفيد 19" تم نشر الكثير من الأخبار عنه وعن كيفيات التعامل معه، وكذلك عن مدى قدرة واستعداد الدولة الجزائرية وهياكلها الصحية للتعامل مع تفشي هذا الوباء والتصدي له، وتم تداول الكثير من الأخبار عن الإهمال في هذه المرافق للمرضى الذين كانوا محتجزين في المستشفيات بغرض الحجر الصحي في بداية تفشي الوباء، وشهدت هذه الفترة أيضًا انتشار شائعات عن نقص بعض المواد الغذائية وتوقع إجراءات وتدابير معينة ستتخذها الدولة، الأمر الذي خلق حالة من انعدام الأمن بين المواطنين وخلق في نفس الوقت حالة من الذعر بينهم إضافة إلى ذلك الذعر الناجم عند ظهور الوباء وتزايد عدد الإصابات يوميا. هذا ما يؤثر على الصحة العامة وأطر مكافحة الأمراض المعدية[1]، فهذه الأخيرة تعتبر عنصر جوهري من عناصر النظام العام، وكذلك هذه الأخبار الكاذبة تمس بالأمن العام الذي يعتبر هو بدوره عنصر جوهري من عناصر النظام العام كونها تزرع في أنفس الأشخاص الرعب وآلاّ إطمئنان على أنفسهم. وبالتالي استوجب على المشرع تجريم هذه الأفعال.

وما يجدر بنا الإشارة إليه أن لوسائل التواصل الاجتماعي دور فعال في نشر الأخبار الكاذبة، من خلال مواقعها التي يتردد عليها الملايين من الأشخاص من جميع الأعمار والطوائف والجنسيات، ويتم تداولها من طرف الأشخاص دون التأكد والتحقق من صحتها،

[1] ربيعة فرحي، المرجع السابق، ص 21.

لتصبح منتشرة بين الكافة، فعلى الرغم من إيجابيات التطور التكنولوجي ووسائل التواصل الإجتماعي بكل مزاياها، إلا أنها بيئة خصبة للمعلومات المغلوطة، والأخبار الكاذبة، مما يؤدي إلى نشر الفوضى والتضليل، ونظرا لعجز الحكومة على السيطرة المطلقة عليها، فإذا ما تم حجب موقع إلكتروني، ظهرت آلاف المواقع التي تنتشر نفس المحتوى، مما يشير إلى أنه ليس من السهل على دولة ما أن تتدخل بحظر الانترنت، أو حجب المواقع جزئيًا أو كليًا، لأن هذا يضع عبئًا ثقيلًا على كاهلها [1].

2_ أركان جريمة نشر وترويج أخبار أو أنباء تمس بالنظام العام والأمن العموميين:

تتكون هذه الجريمة على غرار بقية الجرائم من ثلاث أركان أساسية.

أ_ الركن الشرعي: حيث نصت عليها المادة 196 مكرر من ق.ع.ج التي جاء بها القانون رقم 20-06 لسنة 2020[2].

ب_ الركن المادي: وحسب هذه المادة يتمثل السلوك المجرم في النشر والترويج للأخبار الكاذبة أو المغرضة بأي وسيلة كانت، فالمشرع لم يحدد وسيلة النشر أو الترويج من خلال استخدامه العبارة التالية: "**بأي وسيلة كانت**" يعني وسيلة تقليدية كالكتابة والطباعة والنشر أو وسيلة حديثة إلكترونية كمواقع التواصل الاجتماعي والحسابات الالكترونية، فهذه الجريمة انتقلت من البيئة الواقعية إلى البيئة الرقمية، لتأخذ شكلا جديد من الجرائم المتعلقة بأنظمة

[1] أسامة حسين محي الدين عبد العال، تجريم الشائعات عبر وسائل التواصل الاجتماعي في التشريع الجنائي المصري دراسة تحليلية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين الشمس، مصر، المجلد 63، العدد1، يناير 2021، ص 7- 8.

[2] المادة 196 مكرر من القانون رقم 20_06 المؤرخ في 5 رمضان عام 1441 الموافق 28 أفريل 2020 المعدل والمتمم لقانون للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج، العدد 25 المؤرخة في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020 تنص على أنه " يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000دج، كل من ينشر أو يروج عمدا، بأي وسيلة كانت، أخبار أو أنباء كاذبة أو مغرضة بين الجمهور يكون من شأنها المساس بالأمن العمومي والنظام العام.

تضاعف العقوبة في حالة العود"

المعالجة الآلية للمعطيات، وحسنا فعل المشرع بعدم حصره للوسيلة في الوسائل التقليدية بل جعل هذه الجريمة ترتكب بأي وسيلة وذلك بغرض توسيع دائرة التجريم، حتى لا يفلت مرتكبي هذا النوع من الجرائم الخطيرة الماسة بالأمن والنظام العام. وكذلك لم يبين طبيعة الخبر المنشور إذا كان سياسي أم إقتصادي أم إجتماعي.

وفعل النشر يعني إذاعة الخبر الكاذب للغير[1]، وما يلاحظ كذلك أن المشرع لم يحدد صور النشر إذ يمكن أن يتخذ عدة أشكال منها: النشر على صفحة الجاني الشخصية أي في حسابه الشخصي أو في صفحات لأشخاص أخرين، أو في مجموعات أو صفحات يكون الجاني مدير فيها أو مشرف عليها، والتساؤل هنا يثور حول ما إذا تم النشر للأخبار أول مرة أما إعادة نشرها وهل تقوم المسؤولية ج لمن أعاد نشر خبر كاذب وتطبق عليه هذه المادة؟ والمشرع لم يفصل في هذه المسألة.

أما الترويج: "روج أخبار أي أشاعها وأفشاها، وروج كلامه أي زينه، وراجت الإشاعة أي انتشرت وفشت أو شاعت، ومروج الأخبار هو ناقل القيل والقال، والترويج هنا يقصد به النشر الذي ينطوي على دعاية وليس نقل الأخبار"[2]، والأخبار الكاذبة أو المغرضة: " هي أخبار أو إشاعات مغايرة للحقيقة أو مغرضة أي يهدف الجاني من ورائها إلى غرض آخر غير مجرد التبصير بالحقائق، وتكون شكل دعايات مثيرة تثير في النفوس هياجا وتوترا وإثارة" [3].

فحسب رأينا هي أخبار أو إشاعات غير صحيحة أو منحازة لأطراف، ليس الهدف من وراء نشرها وترويجها، مجرد فهم الحقائق ونقل الخبر، بل تنشر في نفوس الأفراد الخوف وتزعزع استقرار النفوس.

[1] بهاء المري، المرجع السابق، ص 564.

[2] بهاء المري، المرجع نفسه، ص 687-688.

[3] محمد جمال حنفي زينو، المرجع السابق، ص34.

وما يلاحظ أن المشرع الجزائري لم يبين الوسيلة وكذلك شكل النشر إذا كان مكتوب إلكترونيا أو في صور أو تسجيلات صوتية أو تسجيلات فيديو .... الخ، وكذلك مالم يشترط عدد معين من المشاهدات إذا كان فيديو أو عدد معين من الأشخاص المتابعين للصفحة الشخصية للجاني أو الصفحات التي ينشط عليها ويقوم بالنشر فيها.

والمشرع الجزائري اعتبر هذه الجريمة من جرائم الخطر، حيث لم يشترط المشرع تحقق نتيجة إجرامية معينة، كحدوث مظاهرات نتيجة نشر أو ترويج الخبر الكاذب، أو وقوع ضرر فعلي يمس بالمصلحة العامة[1]، فلمجرد إرتكاب السلوك الإجرامي المتمثل في نشر أخبار كاذبة وكان من قوته احتمال إحداث النتيجة المرجوة عاقب القانون صاحب السلوك على جريمة الشائعة ولو لم تتحقق النتيجة، ففي هذه الجريمة المشرع تدخل بالتجريم في لحظة سابقة على تحقق الضرر الفعلي، ومكتفيا لاكتمال الجريمة قانونًا بتحقق الخطر بالنسبة للمصالح المحمية، حيث أن القانون لا يتطلب أن يحدث فعلا تكدير الأمن العام، ألحاق الضرر بالمصلحة العامة...، حيث يتحقق كل ذلك بكل ما من شأنه خلق التوتر وإشاعة الخوف والتذمر بينهم[2]، وهذا يتضح من العبارة التالية "**يكون من شأنها المساس بالأمن العمومي والنظام العام**"، فمن خلال هذه العبارة يتضح أن الضرر في هذه الجريمة محتمل الوقوع وليس محقق.

وحسنًا فعل المشرع لأنه لو كانت هذه الجريمة من جرائم الخطر فإن النتيجة قد تكون خطيرة جدًا لذا المشرع اعتمد على التجريم الوقائي في هذا الشأن تماشيا مع السياسة الجنائية الحديثة.

وما يجدر ذكره في هذا الصدد أن عبارة "المساس بالأمن العمومي والنظام العام " عبارة غير واضحة وغامضة وتتميز بالمرونة. فالمشرع استعمل هذه العبارة وذلك لما ينطوي

[1] شنه محمد، جريمة نشر الأخبار الكاذبة في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 07، العدد01، جوان 2022، ص 357.

[2] أسامة حسين محي الدين عبد العال، المرجع السابق، ص 77- 78.

عليه نشر الأخبار الكاذبة والمغرضة من أثر كبير في زرع الشك والخوف في نفوس المواطنين، وبالتالي هذه الأفعال تؤدي إلى الاعتداء على الطمأنينة التي تعد أحد أهداف النظام العام[1].

وتكون في ذلك السلطة التقديرية لقاضي الموضوع، الذي يقدر إذا ما كان الخبر الكاذب أو المغرض يمس بالنظام العام أم لا حسب المجرى العادي للأمور، فإذا لم تكن هذه الأخبار المنشورة والمروج لها من شأنها أن تمس بالأمن العمومي والنظام العام فإن ناشرها والمروج لها لا تقوم مسؤوليته الجزائية، أما إذا كان العكس فلا تقوم مسؤوليته الجزائية[2].

ولا بد لقيام الركن المادي لجريمة الأخبار الكاذبة والشائعات، أن تكون هناك علاقة سببية بين الفعل المُجَرم والضرر أو الفعل المُجَرم والخطر الذي ينتج عن هذه الاخبار والشائعات الكاذبة، ومفاد ذلك أن النتيجة التي أحدثها السلوك الإجرامي هي التي تؤسس لمسؤولية الفاعل[3].

ويُضاف لهذ الجريمة ركن يتمثل في ركن العلنية والجدير بالذكر بخصوص النشر الإلكتروني أنه يُشترط فيه أن يكون **علانيا**[4]، وعلة ذلك حتى يستهدف عددا من الأفراد بلا تمييز كالنشر في مجموعات إفتراضية[5]، فالمشرع الجزائري رغم أنه لم يذكر صراحة شرط

[1] ربيعة فرحي، أثر الجائحة كوفيد-19 في سياسة التجريم والعقاب في قانون العقوبات الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة، الجزائر، المجلد 58، العدد03، 2021، ص21.

[2] شنه محمد، المرجع السابق، ص 357- 358.

[3] حسون عبيد هجيج، حسن مهدي حمزة، جريمة بث الأخبار والإشاعات الكاذبة، مجلة جامعة بابل للعلوم الانسانية، جامعة بابل، العراق، المجلد26، العدد 7، سبتمبر/ أيلول 2018، ص 255.

[4] تُعرف العلنية لغة: "علن تعني جهُر وانكشاف، عكسه سر"، أما اصطلاحا: هي اتصال علم الأشخاص سواء بقول أو بفعل أو بأي نوع من الكتابة يمكنهم من خلاله معرفة الرأي أو الفكرة المذاعة أو المنشورة. أنظر محمد منصور البابا، تجريم الشائعة في التشريع الأردني (دراسة مقارنة)، قدمت هذه الرسالة إستكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط ، كلية الحقوق، حزيران 2020، ص83.

[5] محمد جمال حنفي زينو، المرجع السابق ، ص 35.

العلنية إلا أنها تترض مدام سلوك النشر والترويج غير موجهة لفئة محددة ويستهدف عامة الناس وبالتالي يكون علنيا.

جـ الركن المعنوي: من خلال ورود مصطلح عمدًا في نص المادة 196 مكرر من ق.ع.ج[1] يتضح أن هذه الجريمة عمدية ولا تكون خطأً، فهي تطلب القصد الجنائي العام، حيث يعلم الجاني بسلوكه الإجرامي المتمثل في نشر أو ترويج الأخبار الكاذبة والمغرضة، ويعلم أن ذلك من شانه المساس بالأمن العمومي والنظام العام، وأن تتجه إرادته لإرتكاب هذا السلوك[2].

أما بالنسبة للعقوبات المقررة لهذه الجريمة هي: الحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000دج، وبالتالي فجريمة نشر الأخبار الكاذبة أو مغرضة بين الجمهور التي من شأنها المساس بالأمن العمومي والنظام العام هي جنحة.

وفي حالة العود فإن العقوبة تضاعف فتصبح من سنتين (2) إلى ستة (6) سنوات والغرامة تصبح من 200.000 دج إلى 300.000 دج.

[1] والتي تنص "...كل من ينشر أو يروج **عمدًا**، بأي وسيلة كانت، أخبار أو أنباء كاذبة أو مغرضة بين الجمهور يكون من شأنها المساس بالأمن العمومي والنظام العام".

[2] شنه محمد، المرجع السابق، ص362- 363.

المبحث الثاني: السياسة التجريمية والعقابية التي اتبعها المشرع الجزائري لمكافحة جرائم المعطيات الشخصية

إن قانون العقوبات أورد الإطار العام للنصوص الموضوعية التي تجرم المساس بأنظمة المعالجة الآلية للمعطيات، فلم نص على حماية معطيات النظام لم يبين نوعية المعطيات، ما إذا كانت معطيات تتصل بالشخص أو بمصالح اقتصادية أو مالية أو مسائل أمنية أو غير ذلك، ومرد ذلك السعي لتعميم الحماية الجنائية للمعطيات بكافة أنواعها بما فيها المعطيات الشخصية، ونظرا لخطورة هذه الأخيرة وحساسيتها فإن القواعد العامة أثبتت في أرض الواقع عدم كفايتها في إقرار حماية جنائية فعالة لهذا النوع من المعطيات، لذا تم تشريع قانون منفصل عن قانون العقوبات متخصصا ومتميزًا، حيث حذا حذو الاتفاقية الأوروبية (إتفاقية بودابست)، التي بدورها أضفت حماية جنائية عامة لكل أنواع العطيات، وذلك لوجود تشريع قائم بذاته وأكثر تميزًا عن التنظيم التشريعي العام لجرائم الكمبيوتر، يتمثل في الاتفاقية الأوروبية لحماية البيانات الشخصية[1].

المطلب الأول: مظاهر حماية المعطيات ذات الطابع الشخصي من المعالجة الآلية

إن المشرع الجزائري كغيره من التشريعات المقارنة لم يحظر معالجة المعطيات الشخصية، وإنما وضع تنظيما قانونيا خاصا بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حدد كيفيات تنفيذ معالجة المعطيات ذات الطابع الشخصي والشروط الواجب توافرها عند القيام بعملية المعالجة.

ومن خلال هذا المطلب سنتطرق إلى مفهوم المعطيات ذات الطابع الشخصي (الفرع الأول)، ومبادئ وضوابط المعالجة الآلية للمعطيات ذات الطابع الشخصي (الفرع الثاني).

[1] مروة زين العابدين صالح، المرجع السابق، ص 440.

الفرع الأول: مفهوم المعطيات ذات الطابع الشخصي

بغرض توضيح الإطار المفاهمي للمعطيات ذات الطابع الشخصي تطرقنا من خلال هذا الفرع إلى تعريفها (أولا)، وأنوعها (ثانيا).

أولا: تعريف المعطيات ذات الطابع الشخصي

1_ التعريف الفقهي:

وقد عرفت البيانات الشخصية لجنة المعلومات والحريات الفرنسية بأنها " بيانات تتخذ شكل جملة إشارة أو رقم أو جملة أو كلمة أو صفة معينة تجعل الشخص قابلا للتحديد"، وتعرف أيضا من قبل الفقه بأنها البيانات الشخصية التي تتعلق بحرمة الحياة الخاصة للإنسان ومنها ما يسمح رسم صورة لاتجاهاته وميوله، ومنها التي تتعلق باتجاهاته السياسية ومعتقداته الدينية وتعاملاته المالية والبنكية وجنسيته وهواياته[1].

وعرف المشرع الجزائري اصطلح عليها تسمية المعطيات ذات الطابع الشخصي وعرفها على أنها "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه "الشخص المعني" بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الإقتصادية أو الثقافية أو الإجتماعي"[2].

---

[1] علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة – دراسة مقارنة–، د.ط، المكتب الجامعي الحديث، الاسكندرية، 2019، ص 95- 96.

[2] أنظر المادة 2 من القانون رقم 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج. ر. ج. ج، العدد 34، المؤرخة في 25 رمضان عام 1439 ل 10 يونيو سنة 2018.

وما يلاحظ أن المشرع الجزائري أخذ بالتعريف الموسع للمعطيات الشخصية وهذا ما يستشف من عبارة "كل معلومة" التي استخدمها المشرع في النص.

وهو ما انتهجه المشرع الفرنسي[1].

ثانيا: أنواع المعطيات ذات الطابع الشخصي

1_ معطيات التعرف على الأشخاص: وهي المعطيات التي تمكن بشكل مباشر أو غير مباشر من تحديد الأشخاص الطبيعيين[2]، وتنقسم إلى نوعين:

أ_ معطيات التعرف المباشر على الأشخاص: هي المعطيات التي تسمح بالتعرف على الشخص مباشرة وتتمثل في: الإسم واللقب، صورة الشخص ولا يهم ذا كانت في شكل ثابت أو متحرك (فيديو)[3]، فهذه الأخيرة وصوت الشخص في البيئة الرقمية، اعتبرتهما اللجنة الوطنية للمعلوماتية والملفات (CNL) الفرنسية معطيات قابلة للمعالجة الآلية[4]، ولجنة الحريات الفرنسية سايرة هذا التوجه الحديث[5]،لأنهما يمكنان من التعرف على الشخص بدون إدراج إسمه أو وجهه[6].

ب_ معطيات التعرف غير المباشر على الأشخاص: معطيات التعرف بصفة غير مباشرة يقصد بها هناك بيانات رمزية بشكل غير مباشر وهي تلك التي تسمح بالتعرف على شخص

[1] عرف القانون الفرنسي البيانات الشخصية في القانون الفرنسي رقم 7 لسنة 1978 المعدل بالقانون رقم 801 لسنة 2004 الخاص بحماية البيانات الشخصية في المادة الثانية منه والتي جاء فيها "يعتبر بيانا شخصيا أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه"

[2] Brigitte van dorsselaere, Guide juridique de l'informatique, Aubin imprimeur, Paris, France, 1990, p87.

[3] نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي –دراسة مقارنة–، مجلة الدراسات القانونية المقارنة، مخبر البحث، "القانون الخاص المقارن"، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 07، العدد01، 2020، ص 1999.

[4] نبيلة رزاقي، المرجع نفسه، ص 1999.

[5] باسم محمد فاضل مدبولي، المرجع السابق، ص 36.

[6] نبيلة رزاقي، المرجع نفسه، ص 1999.

على الرغم من عدم اقترانها بهوية، وتتمثل في أي شكل من أشكال الأرقام الشخصية[1]، كرقم التعريف الوطني، الرقم التأميني، رقم السيارة ، عنوان IP ...، وأي رقم أخر ينفرد به الشخص الطبيعي[2]، إضافة إلى العنوان: ويقصد به في القانون موطن الشخص[3]، فهذه المعطيات تمكن من التعرف على الشخص من خلال التوفيق بين المعطيات المتواجدة في ملف التسجيل وشخص من خلال الربط بينهما[4]، وكل هذه المعطيات قد تكون في القطاع العام أو القطاع الخاص.

2 _ أنواعها وفقا للقانون رقم 18-07:

وتنقسم المعطيات الشخصية إلى معطيات عادية يمكن تطبيق القانون 18-07 بشأنها خلال مرحلة المعالجة ومعطيات حساسة يُحظر معالجتها:

أ_ المعطيات ذات الطابع الشخصي غير الحساسة (العادية):

وتتمثل في كل المعطيات التي يمكن معالجتها وفقا للقانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ماعدا تلك التي حُظر معالجتها صراحة بموجب هذا القانون، أو كانت تخضع لأحكام خاصة لابد من إتباعها حتى تتم عملية معالجتها.

ب_ المعطيات ذات الطابع الشخصي التي يُحظر معالجتها وفقا للقانون 18-07:

_ المعطيات الحساسة: بعض القوانين تسميها معطيات شخصية ذات طبيعة خاصة، وهي فئة من المعطيات الشخصية يكون نطاقها أضيق من نطاق المعطيات الشخصية بشكل عام، ويُحظر جمعها في معظم التشريعات، نظرًا لارتباطها المباشر بالحقوق الأساسية

[1] Guy Marcei Kameni, la vie privée en droit camerounais, thése en vue de l'obtention du doctorat, l`université de toulouse 1 capitole (UT1 capitole) EA1920 en cotutelle internationale avec:l`université de douala (cameroun), 2012/2013, p 179.

[2] باسم محمد فاضل مدبولي، المرجع السابق، ص 38.

[3] باسم محمد فاضل مدبولي، المرجع نفسه، ص42.

[4] Guy Marcei Kameni, ibid, p 179.

المعترف بها في المواثيق الدولية والقوانين الأساسية[1]، وعرفها القانون 18-07 في المادة 3 منه بأنها "معطيات ذات الطابع الشخصي تبين الأصل العرقي أو الإثني أو الأراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني أو تكون متعلقة بصحته بما فيها معطياته الجينية"[2]. وما يجدر بنا الإشارة إليه أنه توجد صعوبة في تحديد وحصر المعطيات الحساسة وتوحيدها في غالبية التشريعات، والمشرع الجزائري حسنًا فعل بتحديدها في المادة السالفة الذكر على سبيل الحصر وليس على سبيل المثال وهذا حتى لا يترك المجال لإدخال أي نوع من المعطيات الأخرى تحت مسمى المعطيات الحساسة والتهرب من معالجتها.

وبالتالي فهو سار على نفس المسار الذي اتبعه المشرع الفرنسي في تحديد هذا النوع من المعطيات[3].

وما يلاحظ أن المشرع الجزائري أورد تعريف ليس دقيقًا، حيث اكتفى بتعريف هذه المعطيات بأنها تبين الأصل والعرق... دون التطرق إلى طريقة كشفها مباشرة أو بشكل غير مباشر، لأن هناك معطيات يمكن معالجتها وهي غير محظورة ومن خلالها يمكن التعرف أو تبين بطريقة غير مباشرة معطيات محظور معالجتها، ولو أعطينا مثال على ذلك أنه مثلا يمكن معالجة صورة للشخص بشكل عادي فالصورة ليست من المعطيات الحساسة، وهذا الشخص يتضح في تلك الصورة أنه يرتدي قلادة بها رسومات أو رموز تبين دينه مثلا أو

[1] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 81.

[2] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] Voir, article *8.* – I. loi n° LOI no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés « Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. »

أصوله العرقية، أو كان يرتدي قميص به صور كذلك أو رموز تبين ما سبق ذكره أو تبين انتماءاته السياسية فهنا يكون الإشكال.

_ المعطيات الصحية: أطلق عليها المشرع الجزائري تسمية المعطيات في مجال الصحة والتي عرفها في المادة 3 من القانون 18-07 على أنها تتمثل في "كل معلومة تتعلق بالحالة البدنية أو العقلية للشخص المعني، بما في ذلك المعطيات الجينية"[1]، وهذه الأخيرة عرفها بأنها " كل معطيات متعلقة بالصفات الوراثية لشخص أو عدة أشخاص ذوي القرابة"[2]، وصنف القانون 18-07 المعطيات الصحية ضمن المعطيات الحساسة، لارتباطها بخصوصية كل شخص طبيعي، إذ لا يمكن الكشف عنها إلا لمن يثق به هذا الشخص، أو لأجل الحصول على مساعدة في مواجهة وضع صحي أو حالة مزعجة مثلا المعطيات الصحية للمرضى في جائحة كوفيد 19، أضف إلى ذلك هذه البيانات مرتبطة بالسلامة الجسدية والعقلية والنفسية، لذا فيمكن أن تؤثر مباشرة على المستقبل المهني والعائلي أو الحالة الإجتماعية للفرد، فمن هنا يتضح حرص المشرع على حمايتها حماية خاصة[3].

والمشرع الجزائري في القانون 18-07 جعل **المبدأ العام هو حظر** معالجة هذه البيانات، لكن **إستثناءا يمكن معالجتها**، حيث نصت المادة 5 من القانون 18-07 أنها تخضع لأحكام هذا القانون المعالجات الآلية للمعطيات ذات الطابع الشخصي الصحية والتي الغاية البحث عن الوقاية والعلاج، مثل دراسة المعطيات المرتبطة بالعلاج والوقاية، وكذلك تقييمها وتحليلها[4]، وبالتالي يمكن معالجة هذا النوع فقط من المعطيات الصحية.

---

[1] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] باسم محمد فاضل مدبولي، المرجع السابق، ص 76.

[4] أنظر المادة 05 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

وهذه المعطيات التي يكون الغرض منها بحث ودراسة وتقييم وتحليل المعطيات المرتبطة بنشاطات العلاج أو الوقاية ورد عليها كذلك إستثناءا لا يمكن معالجة بعضها[1].

الفرع الثاني: مبادئ وضوابط المعالجة الآلية للمعطيات ذات الطابع الشخصي

حدد المشرع الجزائري مبادئ وضوابط المعالجة الآلية للمعطيات الشخصية في القانون 18-07 المتعلق بحماية الأفراد بغرض إرساء نظام تشريعي متكامل الضوابط، وذلك حتى لا يتم الاعتداء على هذا النوع من المعطيات خلال عملية المعالجة، ولا يتم المساس بحقوق الشخص المعني الذي ستكون معطياته محل عملية المعالجة، وهذا يتجسد من خلال مجموعة من الالتزمات الملقاة على عاتق القائم بعملية المعالجة الآلية للمعطيات ذات الطابع الشخصي، لذا فإن من خلال هذا الفرع سنتطرق إلى مشروعية المعالجة كشرط مبدئي واجب التوفر في عملية معالجة المعطيات ذات الطابع الشخصي (أولا)، حقوق الشخص المعني بالمعالجة وإلتزامات القائم بها (ثانيا).

أولا: مشروعية المعالجة كشرط مبدئي واجب التوفر في عملية معالجة المعطيات ذات الطابع الشخصي

بادئ ذي بدء وجب علينا أن نتطرق إلى تعريف معالجة المعطيات ذات الطابع الشخصي، والتي أوردها المشرع الجزائري في المادة الثالثة من القانون 18-07 حيث عرفها بأنها تتمثل في "كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو

[1] أنظر المادة 05 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

أي شكل آخر من أشكال الإتاحة أو التقريب أو **الربط البيني**[1]، وكذا الإغلاق أو التشفير أو المسح أو الإتلاف"[2]، وهو نفس التعريف الذي نص عليه المشرع الفرنسي في المادة 02 من قانون حماية البيانات الشخصية[3].

وما يلاحظ أن المشرع الجزائري لم يستثني الطرق اليدوية للمعالجة، وأورد لنا عدة أمثلة في هذه المادة فلم يحصر عملية المعالجة فيما ذُكِر فيه فقط.

يجب أن تكون معالجة المعطيات ذات الطابع الشخصي مشروعة، ولمشروعية المعالجة لابد من توافر مجموعة من المبادئ الأساسية لعملية المعالجة وتتمثل في:

1_ مبدأ الموافقة المسبقة لصاحب المعطيات:

فالموافقة الصريحة لصاحب المعطيات تعتبر شرط أساسي للقيام بمعالجة المعطيات الشخصية، وما يجب الإشارة إليه أن موافقة صاحب المعطيات ليست نهائية، حيث يمكنه التراجع عليها في أي وقت، وإستثناءًا موافقة صاحب المعطيات المعني لا تكون واجبة إذا كانت المعالجة ضرورية، وذلك في حالة الامتثال للالتزام القانوني، ولحماية حياة الشخص صاحب المعطيات، وكذلك في حالة تنفيذ عقد يكون صاحب البيانات طرفًا فيه، أو لتنفيذ إجراءات تعاقدية سابقة تم اتخاذها بناءً على طلب صاحب هذه المعطيات، ولحماية مصالح

[1] الربط البيني للمعطيات: يتمثل في أي شكل من أشكال المعالجة يهدف إلى إنشاء رابط بين المعطيات التي تتم معالجتها لأغراض محددة مع معطيات الأخرى التي يحتفظ بها مسؤول أو أكثر عن المعالجة أو يمسكها نفس المسؤول للغرض ذاته أو لأغراض أخرى. أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] Art 02 « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction… » modifié par loi N° 801-2004 du 6 aout 2004- Art 1 , JORF 7 aoùt 2004.

صاحب البيانات، إذا كان ليس له القدرة للتعبير عن موافقته، للقيام بمهمة تندرج في إطار مهام المصلحة العامة أو ممارسة وظائف السلطة العامة التي يمارسها المراقب أو طرف ثالث على علم بالبيانات أو لتحقيق المصالح المشروعة للمسؤول عن المعالجة أو المرسل اليه، ويتم في هذا الشأن مراعاة مصالح صاحب المعطيات حقوقه وحرياتهم الأساسية[1].

وإذا كان صاحب هذه المعطيات عديم الأهلية أي صغير في السن أو مجنون، أو ناقص الأهلية (سفيه، ذي غفلة)، فإن موافقته تخضع للقواعد العامة المنصوص عليها في القانون، فبالنسبة **للطفل**[2] فإن المشرع الجزائري حظر معالجة معطياته الشخصية مباشرة إلا بعد الحصول على موافقة **ممثله الشرعي**[3] والمتمثل في ولي الطفل أو وصيه...، أو عند الاقتضاء بترخيص من القاضي المختص، ويمكن لهذا الأخير أن يأمر بمعالجة هذه المعطيات، حتى إذا لم يتحصل على موافقة ممثله، إذا اقتضت **المصلحَةُ الفُضْلَى**[4] للطفل ذلك. ويمكنه كذلك العدول عن ترخيصه في أي وقت[5]، ومصطلح المصلحة الفضلى للطفل

[1] أنظر المادة 7 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] تنص المادة 2 في فقرتها الثانية من القانون رقم 15- 12 المؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015 المتعلق بحماية الطفل، ج.ر.ج.ج، العدد 39، الصادرة بتاريخ 3 شوال عام 1436 هـ الموافق 19 يوليو سنة 2015، على تعريف الطفل بأنه: " كل شخص لم يبلغ الثامنةَ عَشَرَ 18 سنة كاملة"

[3] تنص المادة 2 من القانون رقم 15- 12 المتعلق بحماية الطفل على أن "الممثل الشرعي للطفل: وليه أو وصيه أو كافله أو المقدم أو حاضنه".

[4] تنص المادة 7 من نفس القانون السالف الذكر على أنه: " يجب أن تكون المصلحة الفضلى للطفل الغاية من كل إجراء أو تدبير أو حكم أو قرار قضائي أو إداري يُتخذ بشأنه.

يؤخذ بعين الاعتبار، في تقدير المصلحة الفضلى للطفل، لاسيما جنسه وسنه وصحته واحتياجاته المعنوية والفكرية والعاطفية والبدنية ووسطه وجميع الجوانب المرتبطة بوضعه."

[5] أنظر المادة 8 من القانون 18-07 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

مصطلح يُفسر ويتم تأويله حسب وجهة نظر كل طرف، ويلزم التعامل معه بحذر وفقا للمنظور الوطني والحضاري للمجتمع الذي يعيش فيه الطفل[1].

2_ مبدأ مشروعية ونزاهة المعالجة:

يعتبر هذا المبدأ أحد أهم مبادئ عملية المعالجة، فالمشروعية (Licite) تعني أن عملية المعالجة تكون وفقا لما يتطلبه القانون، أما النزاهة (Loyale) فهي تتضمن على تقدير معنوي وأخلاقي أكثر من كونه قانوني، وتخضع للسلطة التقديرية للقاضي المختص[2]، فقانون المعطيات الشخصية يتطلب أن تكون المعالجة مشروعية، وهذا الشرط جاء عاما غير واضح ودقيق لم يحدد الأساس القانوني الواجب الإستناد عليه حتى تكون هذه المعالجة مشروعة، وهذا خلافا لبعض التشريعات التي حددته. ومثالها الائحة العامة لحماية البيانات (GDPR) في المادة 6 منها في فقرتها الأولى نصت على الأسباب المشروعة للمعالجة. حيث إذا تخلفت هذه الأسباب تعتبر المعالجة غير مشروعة.

3_ مبدأ الغائية من تجميع المعطيات ومعالجتها[3]:

عند إجراء عملية المعالجة لابد من تجميع المعطيات، وهذه المعطيات لابد أن تكون مجمعة لغايات وأغراض محددة، وواضحة ومشروعة، ويجب أن لا تتم معالجتها لاحقا بطريقة لا تتماشى الغايات التي جُمعت من أجلها[4]، وهذا المبدأ يتطلب لتنفيذ أي معالجة للبيانات الشخصية وجود غرض محدد بدقة وواضحا بشكل كافٍ، وأغراض أخرى إضافية متوافقة مع الغرض الأولي إن وجدت أغراض متعددة، وتعتبر غير قانونية معالجة المعطيات

[1] نجيمي جمال، قانون حماية الطفل في الجزائر تحليل وتأصيل، ط 2، دار هومه، الجزائر، 2016، ص 49.

[2] فتيحة حزام، إجراءات المعالجة الآلية للمعطيات ذات الطابع الشخصي وفقا لأحكام القانون 18-07، مجلة البحوث والدراسات الإنسانية، جامعة 20 أوت 1955، سكيكدة، الجزائر، المجلد 15، العدد 01، 2021، ص 347.

[3] مبدأ الغائية من تجميع المعطيات ومعالجتها ويطلق عليه كذلك تسمية مبدأ تحديد الغرض من تجميع المعطيات ومعالجتها (Principe de la limitation de la finalité).

[4] أنظر المادة 9 من القانون من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

التي يُفترض أن تكون مفيدة في وقت ما في المستقبل، إضافة إلى ما سبق يجب إن كانت هناك أغراض جديدة للمعالجة أن تتوافق مع الغرض الأصلي لأن المعالجة تقتصر على الغرض المحدد في البداية، وبذلك أي غرض جديد سيتطلب أساسا قانونيا، فمراقب عملية المعالجة حتى يكون هناك توافق لابد عليه أن يأخذ في الإعتبار كل ربط بين هذه الأغراض وأغراض المعالجة الإضافية المقدمة[1].

4_ مبدأ التناسبية:

وفقًا لهذا المبدأ يجب أن تكون المعطيات الشخصية ملائمة ومناسبة وليست مفرطة بالنسبة إلى الغايات التي تم جمعها ومعالجتها من أجلها، فيجب أن تستند كل معالجة على معطيات تجمعها علاقة مباشرة بالغايات المحددة في بداية المعالجة، ويجب بالإضافة إلى ذلك أن تكون غير مفرطة مقارنةً مع الغايات المذكورة، وأن تكون دقيقة وصحيحة، ما يضمن عدم صدور حكم، أو تقييم خاطئ على صاحبها من جهة، ويضمن مصداقية نتائج هذه المعالجة من جهة أخرى[2]، وحتى تكون البيانات دقيقة وصحيحة لابد من تصحيحها وتحديثها وتحيينها كلما تطلب الأمر ذلك[3]، وبالتالي يتضح لنا أنه حتى يتحقق مبدأ التناسبية لابد من تحقق شرطين أساسيين وهما: شرط تقليل المعطيات وشرط دقة المعطيات اللذان تم النص عليهما في لائحة حماية البيانات بالإتحاد الأوربي (GDPR) كمبدئيين أساسيين مستقلين عن بعضهما من مبادئ معالجة المعطيات، لكن بقراءتنا للفقرة ج من المادة 9 من القانون 18- 07 التي نصت "ملائمة ومناسبة وغير مبالغ فيها بالنظر إلى الغايات التي من أجلها تم جمعها ومعالجتها"، فنلاحظ أن المشرع أدرج المبدئين السابقين الذكر تحت مبدأ واحد وهو مبدأ التناسبية.

[1] Manuel de droit européen en matière de protection des données, Édition 2018 European, p137- 138.

[2] حزام فتيحة، المرجع السابق، ص 348.

[3] أنظر الفقرة د من المادة 9 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

5_ مبدأ محدودية مدة الحفظ[1]:

يجب أن يكون الإحتفاظ بالمعطيات الشخصية على نظام المعالجة الآلية الإلكتروني لمدة محددة، لذلك غالبية التشريعات المقارنة نصت على ضرورة التقيد بالمدة المحددة اللازمة لتحقيق الغاية أو الغرض من تسجيل المعطيات الشخصية على جهاز الحاسب الآلي[2]. ونص المشرع الجزائري في الفقرة (هـ) من المادة 9 من القانون 18- 07 على كيفية حفظ البيانات ومدة حفظها فمن خلال قراءة هذه الفقرة يتضح لنا أنه بمجرد الإنتهاء من المعالجة وتحقق الغرض المرجو من جمع هذه المعطيات لابد من حذفها وعدم الاحتفاظ بها، ويتم حذفها كذلك حتى لو لم يتحقق الغرض أو الهدف من تجميعها ومعالجتها في حالة ما إذا إنتهت المدة المحددة للمعالجة، أو مدة إنجاز الغرض الذي تم تجميعها ومعالجتها من أجله هذا هو المبدأ، والإستثناء الوارد عليه يتمثل في الإحتفاظ بتخزين هذه المعطيات حتى بعد تجاوز المدة المحددة للتخزين، بشرط الحصول على إذن من السلطة الوطنية، بعد تقديم طلب من المسؤول عن المعالجة عندما تكون هناك مصلحة مشروعة[3].

ثانيا: حقوق الشخص المعني بالمعالجة وإلتزامات القائم بها

1_ حقوق صاحب المعطيات وفقا للقانون 18-07:

أ_ تعريف صاحب المعطيات: هو أحد أطراف عملية المعالجة، وهو أكثر الأطراف حرصا على المحافظة على سرية وخصوصية معطياته[4]، والمشرع الجزائري أطلق عليه تسمية الشخص المعني وعرفه في الفقرة الثانية من المادة الثالثة من القانون 18-07 بأنه "كل

---

[1] مبدأ محدودية مدة الحفظ: (Le principe de la limitation de la durée de conservation) ، ويصطلح عليه كذلك مبدأ تأقيت التخزين.

[2] علي عبود جعفر، المرجع السابق، ص 437-438.

[3] أنظر الفقرة (هـ) من المادة 9 من القانون من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] باسم محمد فاضل مدبولي، المرجع السابق، ص 89.

شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة"[1]، وهو نفس التعريف الذي جاء به المشرع الفرنسي[2]، لكن المشرع الجزائري حدد الشخص الذي تتعلق به المعطيات ذات الطابع الشخصي موضوع المعالجة بأنه يتمثل في كل شخص طبيعي، وهذا خلاف للمشرع الفرنسي الذي اكتفى بمصطلح الشخص فقط، ولم يحدد ما إذا كان شخص طبيعي أو معنوي.

ب_ حقوق صاحب المعطيات:

وتم النص على هذه الحقوق في الباب الرابع تحت عنوان "حقوق الشخص المعني"

_ الحق في الإعلام: تم النص عليه في الفصل الأول من الباب الرابع وتحديدًا في المادة 32 من نفس القانون السابق ذكره، حيث يحق له أي لصاحب المعطيات معرفة الجهة التي قامت بتخزين معلوماته، لأنه قد يكون عرضة لتخزين معطياته دون علمه بذلك، وبالتالي يصبح غير عالم بما يحدث بشأن نتيجة تخزين معطياته التي قد تكون صحيحة أو خاطئة، ويتجسد هذا الحق من خلال إلزام الشخص المسؤول عن عملية التخزين بإعلامه بأنه تم تخزينها، ويجب أن يعلم بجميع تفاصيل تلك المعطيات، هذا ما يقلل من إمكانية إساءة إستخدام معطياته الشخصية[3]. وكقاعدة عامة يجب على المسؤول على عملية المعالجة أو ممثله أن يقوم بالإعلام المسبق للشخص الذي يتم الاتصال به لغرض جمع معطياته الشخصية بطريقة واضحة وصريحة لا لبس فيها، حيث يتم إعلامه بهوية الشخص المسؤول عن المعالجة وهوية ممثله إذا تطلب الأمر ذلك، ويتم إعلامه كذلك بأغراض المعالجة، وبأي

[1] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] Voir, article. 2. loi n° LOI no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés « La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement ».

[3] نعيم مغبغب، نعيم مغبغب، مخاطر المعلوماتية والأنترنت – المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن –، د.ط، د.د. ن، د،ب،ن، 1998، ص 251.

معلومة أخرى مفيدة، كحقوقه ونقل معطياته إلى بلد أجنبي، وعن إمكانية نشر وتداول هذه المعطيات في شبكات الانترنت إذا ما تم جمعها في شبكات مفتوحة، في غياب ضمانات الحماية، وكذلك إمكانية تعرضها للقراءة والاستعمال غير المرخص من قِبل الغير[1].

وورد على هذه القاعدة العامة إستثناء، حيث أن إلزامية الإعلام لا تطبق في حالة ما إذا تعذر إعلام الشخص المعني، عند معالجة هذه المعطيات لأغراض إحصائية أو تاريخية أو علمية، مع وجوب إشعار السلطة الوطنية عن هذه الاستحالة من طرف المسؤول عن المعالجة، مع تبرير هذه الإستحالة، أضف إلى ذلك لا تطبق إلزامية الإعلام إذا تمت المعالجة تطبيقا لسند قانوني، أو إذا تمت حصرا لأغراض صحفية أو فنية أو أدبية[2].

وهذا الحق يمهد إلى تمتع صاحب المعطيات بحق أخر وهو الحق في الإطلاع والذي يمثل نتيجة مباشرة لهذا الحق، وبالمفهوم العكسي فإن الحق في الإطلاع يصبح دون فائدة إذا لم يكون الشخص على علم بالمعطيات المخزونة عنه.

ـ الحق في الإطلاع على المعلومات والوصول إليها: وتم تعريف هذا الحق بأنه إمكانية حصول الأفراد على المعلومات والبيانات من المؤسسات والاطلاع على السجلات ذات الصلة[3]. فمن الطبيعي أن يكون لصاحب المعطيات الحق في الإطلاع على المعلومات المتعلقة به لأنها تخصه وحده دون غيره، ويكون هذا الإطلاع بناءًا على طلب خطي يقدمه صاحب البيانات كتابة أوشفاهة[4]، ويجب إعطاء هذا الشخص صورة صحيحة عن المعلومات المخزونة عنه سواء كانت في القطاع العام أو الخاص[5].

---

[1] أنظر المادة 32 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 33 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] باسم محمد فاضل مدبولي، المرجع السابق، ص 90.

[4] باسم محمد فاضل مدبولي، المرجع نفسه، ص 90.

[5] نعيم مغبغب، المرجع السابق، ص250.

ـ حق الإعتراض على المعطيات: يعتبر حق الاعتراض من تطبيقات حق الشخص في احترام حرياته الأساسية المتعلقة بمعالجة معطياته الشخصية، فبموجب هذا الحق يجوز لصاحب المعطيات أن يعلن عن رفضه لأي إجراء يتعلق بمعطياته الشخصية، كما يعتبر هذا الحق ضمانة له، لأنه يمنحه الثقة والأمان، فعند جمع معطياته أو الكشف عنها هو يكون على دراية بأنه يمكنه ممارسة حقه في الاعتراض على أي إجراء فيه مساس بمعطياته الشخصية في المستقبل[1]، إذا كانت الأسباب التي جعلته يعترض مشروعة[2]، هذا وفقا لنص المادة 36 من القانون 18-07[3]، وهو ما نص عليه المشرع الفرنسي كذلك[4]. وفي كلاهما لم يتم تحديد فيما تتمثل هذه الأسباب المشروعة، وبالتالي يبقى تقدير مدى مشروعية هذه الأسباب الاعتراض من عدم مشروعيتها خاضعا للسلطة التقديرية لقاضي الموضوع في كل حالة معروضة أمامه على حدة، والهدف من إشتراط هذا القيد هو عدم التعسف في استعمال هذا الحق[5].

واستثناءًا على قاعدة وجوب تقديم مبرر شرعي للاعتراض، يمكن صاحب المعطيات الاعتراض على استعمال معطياته الشخصية لأغراض دعائية أو إعلانية ولاسيما التجارية

---

[1] سامح عبد الواحد التهامي، المرجع السابق، ص 427.

[2] باسم محمد فاضل مدبولي، المرجع السابق، ص 93.

[3] المادة 36 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

تنص في فقرتها الأولى"يحق للشخص المعني أن يعترض، لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي".

[4]Art 38, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés " Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable

actuel du traitement ou celui d'un traitement ultérieur.

Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée

par une disposition expresse de l'acte autorisant le traitement".

[5] سامح عبد الواحد التهامي، المرجع السابق، ص 428.

منها من طرف المسؤول عن المعالجة الحالية واعتبر ذلك سبب كافٍ للاعتراض وفقا لنصت المادة 36 من القانون 18- 07[1]، وذلك دون تقديم مبرر أو سبب شرعي[2].

ويمكن لصاحب المعطيات ممارسة حقه في الاعتراض في جميع مراحل المعالجة، ويمكنه أيضًا ممارسة هذا الحق عن طريق طلبه محو معطياته ويمكنه ممارسته كذلك عبر الانترنت عن طريق اختيار خانة الرفض في نموذج جمع المعطيات الالكتروني[3]، وفي المرحلة اللاحقة لمرحلة جمع المعطيات، يتم الاعتراض عن طريق إرسال رسالة عبر البريد الإلكتروني[4] من طرف صاحب المعطيات إلى المسؤول عن المعالجة أو الاتصال به مباشرة بالهاتف[5]. وبالمقابل صاحب المعطيات لا يمكنه الاعتراض على معالجة معطياته ذات الطابع الشخصي حتى وإن كانت لديه مبررات مشروعة، إذا كانت المعالجة تفي بالتزام قانوني، أو إذا استبعد هذا الحق بموجب إجراء صريح وارد في الوثيقة التي ترخص بالمعالجة، هذا ما تم النص عليه بموجب الفقرة الأخيرة من المادة 36 من القانون 18-07.[6]

[1] أنظر المادة 36 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 148.

[3] منى الأشقر جبور، محمود جبور، المرجع نفسه، ص 148.

[4] ومن التطبيقات القضائية: اعتبرت المحكمة الابتدائية الكبرى بباريس أن إرسال رسائل إلكترونية إعلانية ودعائية إلى شخص ما رغم اعتراضه يشكل انتهاكا لحقه في الاعتراض على معالجة معطياته الشخصية، وأكدت محكمة النقض الفرنسية على أن معالجة المعطيات الشخصية رغم الاعتراضات هي أمر غير مشروع وغير قانوني، واعتبرت المحكمة بأن جمع عناوين البريد الإلكتروني للأفراد بالرغم من اعتراضهم يعتبر أمرا غير مشروع. وأيدت محكمة النقض الحكم بالغرامة على إحدى مستشفيات الأمراض النفسية بسب معالجتها للمعطيات الصحية لبعض المرضى رغم اعتراضهم على ذلك. أنظر: سامح عبد الواحد التهامي، المرجع السابق، ص 429.

[5] منى الأشقر جبور، محمود جبور، المرجع نفسه، ص 148.

[6] المادة 36 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ـ الحق في الولوج: فهذا الحق يخول لصاحب المعطيات المعني بالمعالجة معرفة ما إذا كانت معطياته قد تمت معالجتها أم لا، ومعرف كذلك أغراض المعالجة والأشخاص المرسل إليهم، وله الحق أيضًا في الحصول على معطياته الشخصية التي تخضع للمعالجة، وكذلك معرفة المصادر التي منها تم الحصول على هذه المعطيات[1]، ولصاحبها الحق أيضا في معرفة فئة المعطيات محل عملية المعالجة[2]، إذا ما كانت هذه المعطيات تنتمي لفئة المعطيات العادية أم لفئة المعطيات الحساسة التي أقر لها المشرع بحماية إضافية لمعالجتها. لكن هذا الحق يمكن الاعتراض عليه من قبل المسؤول عن المعالجة إذا كان الطلب تعسفيا، والذي يستشفه من عدد تقديم هذه الطالبات وطابعها المكرر، الذي يثبت ذلك، كما يحق لهذا الأخير أن يطلب من السلطة الوطنية تحديد مدة للرد على طلبات الولوج المشروعة[3]، وهذا في حالة تعدد الطلبات المقدمة إليه، وبالتالي تصعب عليه الإجابة فورا.

وما يلاحظ أن المشرع الجزائري من خلال هذه المادة التي نص فيها عن هذا الحق أعطى فقط هذا الحق للشخص المعني أي صاحب المعطيات بأنه يمكنه هو وحده ممارسة هذا الحق، ولم يحدد ما إذا كان يمكن لصاحب المعطيات تفويض شخص أخر بصفته وكيل عنه إذا صعب عليه القيام بذلك أو في الحالات التي يكون فيها من الضروري القيام بذلك، أو أن يختار الشخص المعني وكيلاً ينوبه للقيام بهذا، وهذا خلافا للتشريعات المقارنة ومثالها

تنص على أنه " ....لا تطبق أحكام الفقرة الأولى من هذه المادة إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا كان تطبيق هذه الأحكام قد استبعد بموجب إجراء صريح في المحرر الذي يرخص بالمعالجة."

[1] العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي، علي كافي، تندوف، الجزائر، العدد 05، ديسمبر 2018، ص 125.

[2] أنظر المادة 34 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 34 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

التشريع المغربي، وكذلك لم ينص المشرع الجزائري على الحالة التي يكون فيها صاحب المعطيات طفل، وهنا يثار التساؤل حول كيفية ممارسه هذا الأخير حقه في الولوج وإجراءات ممارسته له، وكذلك ما إذا كان يمكن لممثله الشرعي أن يحل محله في ممارسة هذا الحق، أو يأذن له بذلك، وكذلك لم يشير المشرع الجزائري في نصوصه القانونية إلى كيفية تقديم هذا الطلب، وهذا خلافا لبعض التشريعات التي نصت على أن الطلب يمكن أن يكون مكتوب أي مكتوب في ورقة سواء باليد أو بالحاسوب أو إلكتروني أي يتم إرساله عن طريق البريد الإلكتروني أو في عين المكان، وأن يكون موضوعه محدد بدقة، كما لم يحدد المشرع الجزائري كذلك البيانات الالزامية التي يجب أن يتضمنها الطلب، ولم يحدد كذلك الآجال القصوة لأجل تلبية طلب الولوج.

ـ الحق في التصحيح: يسري هذا الحق بعد أن يطلع صاحب المعطيات على معطياته المخزنة أو يحصل على نسخة منها، ويحق له إذا علم بأن هناك معطيات خاصة به مخزنة لدى هيئات حكومية أو خاصة[1]، وكانت هذه المعطيات غير صحيحة، ناقصة وغير كاملة، أو غير مناسبة وليست محينة وقديمة[2]، أي تكون هذه المعطيات تتوافق مع ماهو موجد حقيقة، ولا يكون هناك شك في صحتها[3]، فيطلب من المسؤول على معالجتها بأن يقوم بتصحيحها وتعديلها وتحيين القديمة منها التي مرت عليها فترة زمنية طويلة حتى تكون توافق الحقيقة[4]، وهذا الأخير يُلزمه القانون أن يقوم بهذه العملية مجانًا لصالح صاحبها، وقد حدد المشرع الجزائري مدة 10 أيام من تاريخ تقديم الإخطار للمسؤول للمضي قدما في التصحيح[5]، وذلك لحماية هذا الحق من تماطل وإهمال المسؤول عن المعالجة فرض المشرع

[1] نعيم مغبغب، المرجع السابق، ص 250.

[2] منى الأشقر جبور، محمود جبور، المرجع السابق، ص 149.

[3] Alain Hollande, Prartique du droit de l'informatique et de l'internet, sixéme édition, éditions delmas,Belgique, 2008 , P319.

[4] نعيم مغبغب، المرجع نفسه، ص 250.

[5] أنظر المادة 35 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

هذه الأجال المحددة للقيام بالتصحيح وهي أجال معقولة للقيام بهذا الإجراء، وإذا رفض المسؤول عن المعالجة هذا الطلب أو لم يستجب له بالرد عليه خلال المهلة الزمنية المذكورة سابقا، فإنه يحق للمعني تقديم طلب تصحيح إلى السلطة الوطنية، وهذه الأخيرة تكلف أحد أعضائها بإجراء جميع التحقيقات اللازمة، والسعي للتصحيح في أسرع وقت ممكن، وإبلاغ الشخص المعني بنتيجة طلبه، ويجب إبلاغ الغير الذي وصلت إليه هذه المعطيات بكل تعديل أو تحيين للمعطيات، حتى يتماشى هو كذلك مع هذا التحيين، كما كفل المشرع انتقال حق التصحيح والتحديث إلى الورثة الشرعيين في حال وفاة صاحب المعطيات[1].

ـ الحق في منع الاستكشاف المباشر: يُعرف الاستكشاف المباشر بأنه "إرسال أي رسالة، مهما كانت دعامتها وطبيعتها، موجهة سواء للترويج المباشر أو غير المباشر لسلع أو خدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمة"[2]. والمشرع الجزائري يحظر الاستكشاف المباشر الذي يتم من خلال استخدام آلية اتصال أو جهاز استنساخ عن بعد أو بريد إلكتروني أو أي وسيلة أخرى تستخدام تقنية من نفس الطبيعة، بحيث تستخدام بيانات الشخص الطبيعي بأي شكل من الأشكال دون الحصول على موافقته المسبقة[3]. وبالتالي يحق لصاحب المعطيات منع استخدام معطياته في الاستكشاف المباشر بأي وسيلة إذا كانت بدون موافقته، وعليه فهذا الحق يعتبر آلية مهمة تحمي جميع الأشخاص وخاصة عملاء الهواتف النقالة الذين يتلقون يوميًا رسائل دعائية وترويجية ومسابقات وهمية دون معرفة كيفية وصول أرقام هواتفهم إلى المرسلين ودون معرفة هوية المرسل لطلب التوقف

[1] أنظر المادة 35 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي، تامنغست، الجزائر، المجلد 08، العدد 04، 2019، ص 287.

عن إرسال هذه الرسائل[1]، لكن هناك إستثناءًا حالات يُسمح فيه بالاستكشاف المباشر وهي أن يتم عن طريق البريد الإلكتروني، ومن خلال طلب مباشرة البيانات من الشخص المرسل اليه، عند البيع أو تقديم خدمة، إذا كان الاكتشاف المباشر يتعلق بخدمات أو منتجات مماثلة ومشابهة يقوم بتقديمها نفس الشخص الطبيعي أو المعنوي، والتي تشير صراحة ودون لبس فيها إلى المستلم أنه من الممكن الاعتراض مجانًا[2]، وفي جميع الأحوال يجب الإشارة إلى البيانات الصحيحة للمرسل للسماح للمستلم بإرسال طلب لإيقاف هذه الايصالات مجانًا، باستثناء تسديد مصاريف الإرسال. كما يحظر إخفاء هوية الشخص الذي تم تسليم الرسائل إليه، وكذلك ذكر موضوع لا علاقة له بالخدمات المقدمة[3].

2_ المسؤول عن معالجة المعطيات الشخصية:

أ_ تعريف المسؤول عن معالجة المعطيات الشخصية:

المسؤول عن معالجة المعطيات الشخصية (المراقب) عرفه القانون 18-07 بأنه: "شخص طبيعي أو معنوي، عمومي أو خاص أو أي كيان أخر يقوم بمفرده أو بالاشتراك مع الغير بتحديد الغايات من معالجة المعطيات ووسائلها"[4].

ب_ إلتزامات المسؤول عن المعالجة وفقا للقانون 18-07:

_ التزام المعالج بالإخطار بمعالجة المعطيات: هذا الواجب هو مقابل للحق في الإعلام أو الإخبار الذي يتمتع به صاحب المعطيات.

---

[1] العيداني محمد، يوسف زروق، المرجع السابق، ص126.

[2] أنظر المادة 37 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 37 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] أنظر المادة 03 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

_ الالتزام بالمحافظة على سرية المعالجة: وتقتصر هذه السرية على عدد محدود من الأشخاص، ويبقى العلم به محصورًا في مجال محدد ولا يتجاوزه[1]، أما المشرع الجزائري فقد نص على الالتزام بالسرية في المادة 40 من القانون 18-07 حيث ألزم به المشرع الجزائري كلا من المسؤول عن المعالجة والأشخاص الذين اطلعوا خلال ممارسة مهامهم على المعطيات الشخصية حتى بعد الانتهاء من مهامهم، ورتب على مخالفة هذا الالتزام جزاء[2].

_ الالتزام بالمحافظة على سلامة المعالجة: ويطلق عليها كذلك تسمية تأمين المعالجة أو أمان المعالجة كما جاء في اللائحة الأوروبية، فالمشرع الجزائري نص على مجموعة من الإجراءات والتدابير التي تضمن إضفاء حماية على المعطيات الشخصية، وتمنع من تقويض سلامتها، وفرض على المسؤول عن المعالجة بموجب المادة 38 من القانون 18-07 وضع تدابير وإجراءات تقنية وتنظيمية لحماية هذه المعطيات من التدمير والضياع العرضي أو غير المشروع أو النشر أو الوصول غير المصرح به، لاسيما في عندما تتطلب عملية المعالجة إرسال ونقل المعطيات عبر شبكة معينة، فضلا عن الحماية من جميع أشكال المعالجة غير المشروعة، هذا ما أكدت عليه عبارة "يجب" الواردة في نص المادة، ولم يتوقف المشرع عند هذا الحد، بل شدد على أن هذه الإجراءات يجب أن تتضمن مستوى مناسبًا من السلامة والأمان، بسبب المخاطر التي قد تؤثر على عملية المعالجة[3].

_ في إطار معالجة المعطيات ذات الطابع الشخصي المرتبطة بخدمات التوقيع والتصديق الإلكترونيين: يجب الحصول على المعطيات ذات الطابع الشخصي التي يقوم بجمعها مؤدي خدمات التصديق الإلكتروني بهدف تسليم وحفظ الشهادات المرتبطة بالتوقيع

[1] باسم محمد فاضل مدبولي، المرجع السابق، ص 96.

[2] أنظر المادة 40 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] هشام بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 18-07 معالجة معطيات فيروس كورونا _ نموذجا، مجلة أبحاث قانونية وسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، الجزائر، المجلد 06، العدد 01، جوان 2021، ص 231.

الإلكتروني من الأشخاص المعنيين بها مباشرة، وتتم معالجتها وفقا للأغراض والغايات التي جمعت من أجلها. ويمكن مخالفة هذا إلا إذا أعطى الشخص المعني بالمعالجة موافقته الصريحة[1].

ـ في إطار معالجة المعطيات ذات الطابع الشخصي في مجال الاتصالات الإلكترونية: يقوم مقدمو الخدمات الإلكترونية بتبليغ السلطة الوطنية وصاحب المعطيات في حالة حدوث مساس بخصوصيته أو إذا ما تم إتلاف وتدمير أو ضياع أو الوصول غير المصرح به لمعطياته الشخصية، كما أنهم يلتزمون كذلك بتحديد كل الانتهاكات التي تمس بالمعطيات الشخصية من خلال جردها[2]، فيمسك جرد محين حول الانتهاكات المتعلقة بها ويحديد التدابير المتخذة في هذا الشأن، و كل هذا يكون بعد يتم اتخاذ كل الضمانات اللازمة لحماية المعطيات الشخصية من طرف مقدمو الخدمة[3].

ـ التزامات المسؤول عن المعالجة عند نقل المعطيات نحو دولة أجنبية: لا يمكن المسؤول عن المعالجة نقل المعطيات الشخصية إلى دولة أجنبية إلا إذا حصل على ترخيص من السلطة الوطنية، وأن تكون هذه الدولة التي ستُنقل لها المعطيات ضامنة لمستوى مناسبًا من حماية الخصوصية والحريات والحقوق الأساسية للأفراد عند معالجة هذه المعطيات، وتقدر السلطة الوطنية مدى كفاية الحماية التي تضمنها هذه الدولة، اعتمادًا على المتطلبات القانونية المعمول بها في ذلك البلد والتدابير الأمنية المطبقة هناك، فضلاً عن الخصائص المتعلقة بالمعالجة وأغراضها والمدة، وكذلك طبيعة ومنشأ ووجهة البيانات المعالجة، وفي جميع الأحوال يُمنع إرسال المعطيات الشخصية ونقلها إلى دولة أجنبية إذا كان في ذلك

[1] المادة 42 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] العيداني محمد، يوسف زروق، المرجع السابق، ص 126.

[3] العيداني محمد، يوسف زروق، المرجع نفسه، ص 126.

إضرار بالأمن العام والمصالح الحيوية[1]. وإستثناءًا يجوز نقلها في حالة غياب هذه الشروط في حالات محددة على سبيل الحصر إذا كانت الموافقة صريحة من طرف المعني، وإذا كان النقل ضروريا، وإذا تم النقل تطبيقا لاتفاق ثنائي، أو بناء على ترخيص السلطة الوطنية[2].

المطلب الثاني: الآليات الجزائية لضمان تطبيق قواعد حماية المعطيات ذات الطابع الشخصي

رغم نص القانون 18-07 علىكيفيا ت تنفيذ معالجة المعطيات ذات الطابع الشخصي والمبادئ القانونية الواجب توافرها فيها حتى تكون هذه المعالجة مشروعة، والحقوق التي يتمتع بها صاحب هذه المعطيات والالتزامات المفروض قانونا على القائم بعملية المعالجة والمسؤول عنها، إلا أن هذا غير كافٍ لأنه يستلزم مراعاة تطبيق هذه المبادئ الأساسية في عملية المعالجة وتوافر جميع الشروط القانونية لضمان مشروعيتها، إلا أن عدم الامتثال لهذه المبادئ والشروط يرتب جزاء جنائي يمثل ضمانة لتطبيق قواعد حماية المعطيات ذات الطابع الشخصي عند معالجتها، فتجسدت هذه الحماية الجنائية من خلال إرساء قواعد جنائية تضم شق التكليف المحدد لأركان الجرائم المتعلقة بالمعطيات ذات الطابع الشخصي، وشق الجزاء الذي يحدد نوع العقوبة ومقدارها. وعليه من خلال هذا المطلب سنتطرق إلى الجرائم الواقعة على المعطيات ذات الطابع الشخصي (الفرع الأول)، والعقوبات المقررة لقمع الجرائم الواقعة على المعطيات ذات الطابع الشخصي (الفرع الثاني).

[1] أنظر المادة 44 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 45 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفرع الأول: الجرائم الواقعة على المعطيات ذات الطابع الشخصي

نص القانون 18-07 على الإعتداءات الواقعة على المعطيات ذات الطابع الشخصي في مجال معالجتها، والتي سنتعرض لها كما يلي:

أولا: الجرائم المتعلقة بالمسؤول عن معالجة المعطيات ذات الطابع الشخصي

1_ جرائم انتهاك المسؤول عن المعالجة لشروط معالجة المعطيات ذات الطابع الشخصي:

أ_ جرائم الجمع والتخزين غير المشروع للمعطيات الشخصية: نصت على هذه الجريمة المادة 59 من القانون 18-07، أن السلوك الإجرامي في هذه الجريمة يتمثل في الجمع أو التسجيل أو الحفظ أو تخزين أو معالجة المعطيات الشخصية على نحو غير مشروع[1]، وبطريق الغش والتدليس، كما لو كان الجاني قد تحصل على هذه المعطيات عن طريق التصنت على المكالمات الهاتفية أو التجسس، أو توصيل أسلاك بطريقة خفية إلى الحاسب الآلي الذي تم تخزين البيانات الشخصية في ذاكرته وما شابه[2]، أو المعاملات المتعلقة بالبريد الإلكتروني مثل اعتراض الرسائل الإلكترونية[3]. هذه الجريمة هي جريمة شكلية، يتطلب فيها تحقق السلوك المادي، وهذا لما تنطوي عليه من خطورة إجرامية، لهذا فهي جريمة عمدية، يتخذ ركنها المعنوي شكل القصد الجنائي المفترض، حيث يجب أن يكون الجاني على علم بأن المعطيات محل المعالجة شخصية، بالإضافة إلى علمه بعدم مشروعية جمعها، ويجب أيضًا أن تتجه إرادة الجاني إلى القيام بهذه السلوكات المُجَرمة، وإلا فإنه ينتفي القصد الجنائي لدى الجاني، وبالتالي يتم إنتفاء الركن المعنوي[4].

---

[1] علي عبود جعفر، المرجع السابق، ص 442.

[2] علي نعمة جواد الزرفي، المرجع السابق، ص 103.

[3] هشام بخوش، المرجع السابق، ص 229.

[4] ملياني عبد الوهاب، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 07/18، مجلة البحوث القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، أفلو، الجزائر، المجلد 06، العدد 01، 2023، ص276-278.

ب_ جرائم معالجة المعطيات الحساسة دون الحصول على موافقة صاحب المعطيات: يتمثل السلوك الإجرامي في هذه الجريمة في جمع المعطيات الحساسة التي تقتضي طبيعتها عدم جمعها، دون موافقة الشخصي المعني[1]، يتخذ الركن المعنوي صورة القصد الجنائي بعنصريه حيث يجب أن يعلم الجاني بأن الأفعال التي يقوم بها تشكل معالجة لمعطيات ذات طابع شخصي، وأن المعطيات التي يعمل على معالجتها تشكل معطيات حساسة، وأنه يجري المعالجة المذكورة دون الحصول على موافقة صريحة من الشخص المعني[2].

ج_ جريمة الإحتفاظ بالمعطيات الشخصية أكثر من المدة القانونية اللازمة: نصت عليها المادة 65 من القانون 18-07، تمثل السلوك الإجرامي في هذه الجريمة في الاحتفاظ بالمعطيات الشخصية لمدة تزيد عن المدة المطلوبة، أو المذكورة مسبقًا في الإخطار دون الحصول على الموافقة من السلطة المختصة[3]. وهذه الجريمة عمدية، يأخذ الركن المعنوي فيها صورة القصد الجنائي العام، بتوافر عنصريه العلم والإرادة، وبالتالي لا تقوم هذه الجريمة عن طريق الخطأ، أما في الحالة التي يكون فيها الاحتفاظ بهذه المعطيات الشخصية عن طريق الإهمال والنسيان، فلا يتوفر هنا الركن المعنوي، وفي هذه الجريمة لا يُشترط توافر القصد الجنائي الخاص[4].

د_ جريمة الانحراف عن الأغراض أو الغايات من المعالجة الآلية للمعطيات الشخصية: ونص عليها المشرع الجزائري في المادة 58 من القانون 18-07، ويتوافر الركن المادي في هذه الجريمة عندما ينحرف الجاني عن الغاية أو الغرض الأساسي[5] من عملية المعالجة

[1] سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا «دراسة مقارنة»، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين الشمس، مصر، المجلد62، العدد 1، جانفي 2020، ص117.

[2] سليم محمد سليم حسين، المرجع نفسه، ص161.

[3] علي نعمة جواد الزرفي، المرجع السابق، ص 107.

[4] علي نعمة جواد الزرفي، المرجع نفسه، ص 108.

[5] علي نعمة جواد الزرفي، المرجع نفسه، ص 105- 106.

الذي تم تحديده بعد تجميع أو تخزين المعطيات[1]، والذي تم التصريح به، ومعيار تحديد الانحراف من عدمه هو محتوى الطلب المُقدم إلى الجهة الرقابية التي أصدرت الموافقة والمتمثلة في السلطة الوطنية لحماية المعطيات الشخصية[2]، حيث يتضمن هذا الأخير مُجمل غايات المعالجة[3]، ويتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام الذي يجب توافر عنصريه العلم والإرادة، حيث يكون هنا الجاني على علم من أن السلوك الذي قام به يشكل انحرافا عن الغاية أو الغرض من معالجة المعطيات الشخصية إلكترونيا الوارد في التصريح أو الترخيص الممنوح له، وأن تتجه إرادته نحو ذلك، ولا عبرة بالبواعث التي تدفع الجاني لارتكاب هذه الجريمة أو الغاية التي يهدف إليها، سواء تمثلت بمنفعة للجاني أو دفع ضرر عنه، أو تحقيق مصلحة للغير[4].

[1] بن يوسف القينعي، الجرائم المتعلقة بالإستغلال غير المشروع للمعطيات الشخصية على ضوء القانون: 18-07، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الانسانية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 4، جويلية 2021، ص504.

[2] وفي القانون الفرنسي تتمثل هذه الجهة في اللجنة الوطنية المعلوماتية والحريات العامة (CNIL)

[3] علي نعمة جواد الزرفي، المرجع السابق، ص 105-106.

[4] علي عبود جعفر، المرجع السابق، ص 456.

2_ الجرائم الناجمة عن مخالفة المسؤول عن معالجة المعطيات ذات الطابع الشخصي لالتزاماته:

أ_ جريمة معالجة المعطيات ذات الطابع الشخصي دون الحصول على التصريح أو ترخيص: نص على هذه الجريمة المشرع الجزائري بموجب المادة 56 من القانون 18-07[1]، وذلك بعدم احترام شروط المادة من نفس القانون 12 من نفس القانون، حيث يتحقق الركن المادي لهذه الجريمة بتوافر السلوك الإجرامي وهو كل فعل يتمثل في المعالجة الإلكترونية للمعطيات الشخصية[2]، دون مراعاة الإجراءات الأولية التي يتطلب القانون توافرها[3]، والمتمثلة في عدم الحصول على موافقة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي من خلال الإذن أو التصريح[4]، وهذا يتنافى مع ما نص عليه المشرع الجزائري من وجوب إخضاع كل معالجة للمعطيات الشخصية لترخيص من طرف السلطة التي سبق ذكرها، إلا في الحالة التي يوجد فيها نص قانوني ينص على خلاف هذا[5].

وما يجدر الإشارة إليه أن هذه الجريمة تقوم بمجرد بداء عملية المعالجة من قِبل القائمين بها، في الحالة التي لم يتحصلوا فيها على ترخيص، وتقوم كذلك في الحالة التي

---

[1] المادة 56 من من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي تنص على أنه: " يعاقب بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج إلى 500.000 دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات طابع شخصي دون احترام الشروط المنصوص عليها في المادة 12 من هذا القانون..."

ونصت المادة 12 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي على ما يلي: "ما لم يوجد نص قانوني يقضي بخلاف ذلك، تخضع كل عملية معالجة معطيات ذات طابع شخصي **لتصريح مسبق لدى السلطة الوطنية أو لترخيص** منها طبقا للأحكام المنصوص عليها في هذا القانون."

[2] علي نعمة جواد الزرفي، المرجع السابق، ص 99.

[3] علي عبود جعفر، المرجع نفسه، ص 453.

[4] علي نعمة جواد الزرفي، المرجع السابق، ص 99.

[5] أنظر المادة 12 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

يتم فيها سحب الترخيص أو إلغائه أو تنتهي مدته وتتم مواصلة واستمرار عملية المعالجة[1]، وكذلك في الحالة التي تتم فيها المعالجة بناءًا على تصريح كاذب[2]، وتعتبر هذه الجريمة من الجرائم العمدية[3] التي لابد من توافر القصد الجنائي العام فيها، الذي يقوم على عنصرين أساسيين وهما العلم والإرادة[4]، فالجاني في هذه الجريمة يجب أن يعلم أن هذه المعطيات شخصية، وأن تتم عملية المعالجة الالكترونية دون ترخيص من السلطة المختصة[5].

ب_ جريمة السماح لغير الأشخاص المؤهلين بالولوج لمعطيات ذات طابع شخصي: السلوك الإجرامي في هذه الجريمة يتمثل في السماح لغير الأشخاص المؤهلين قانونا بالدخول إلى المعطيات، لأن إطلاع الأشخاص غير مؤهلين على المعطيات الشخصية يعتبر شرط أساسي لقيام الجريمة، وفي غيابه تنتفي الجريمة[6]، وتكون هذه الجريمة باتخاذ أي سلوك يفيد التعبير عن قبوله بأن يستطيع الغير الاطلاع على هذه المعطيات، ويكون ذلك بأساليب مختلفة منها منح كلمة السر للدخول إلى نظام المعالجة الآلية للمعطيات، أو من خلال ترك النظام مفتوحا لتسهيل الوصول اليه واطلاع الغير عليه، أو بكشف الإجراءات الفنية التي تمنع الولوج للغير، أو عدم التدخل بالاعتراض على الدخول للمعطيات رغم العلم بذلك. وما يلاحظ أن السلوك هنا يمكن أن يكون إما سلبي أو إيجابي، ومصطلح

---

[1] علي عبود جعفر، المرجع السابق، ص 452-453.

[2] الفقرة 2 من المادة 12 من نفس القانون تنص على أنه "...ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له". وما يجدر الإشارة إليه إن هناك من التشريعات التي نصت على جريمة مواصلة المعالجة بعد سحب الترخيص أو التصريح والقيام بتصريحات كاذبة كجريمة مستقلة.

[3] والمشرع الفرنسي يقيم المسؤولية الجنائية في هذه الجريمة أيا كانت صورة الركن المعنوي فيها، وهو ما أكدته محكمة النقض الفرنسية حين اعتبرت هذه الجريمة من الجرائم المادية التي تعترض توافر الخطأ غير العمدي فيها بمجرد إرتكاب الفعل. علي نعمة جواد الزرفي، المرجع السابق، ص100.

[4] علي نعمة جواد الزرفي، المرجع نفسه، ص 100.

[5] علي عبود جعفر، المرجع نفسه، ص 454.

[6] طباش عزالدين، المرجع السابق، ص 56.

الولوج غالبا ما يستخدم عند إجراء معالجة آلية للمعطيات وهو يعني الإطلاع على المعطيات من خلال الدخول آليا لنظام المعالجة الذي يحتوي عليها، وبالتالي يثار اللبس هنا حول ما إذا كان هذا النص يطبق في حالة المعالجة الآلية فقط دون اليدوية، لذا يُستحسن تغييره إلى مصطلح الإطلاع إذا كان المشرع يقصد النوعين معًا من المعالجة[1].

وهذه جريمة من الجرائم العمدية كونها تتطلب القصد الجنائي العام، الذي يقوم على عنصري العلم والإرادة، أما إذا كان الجاني لا يعلم أن الغير الذي أتاح له الولوج غير مؤهل للإطلاع على هذه المعطيات، فهنا لا تقوم هذه الجريمة، وإنما تقوم مسؤوليته الجنائية على جرائم أخرى إذا توافرت أركانها مثل جريمة خرق إلتزامات سرية وسلامة المعطيات المنصوص عليها بموجب المادة 65 من القانون 18-07[2].

ج_ جريمة الإفشاء غير المشروع للمعطيات الشخصية: منصوص عليها بموجب المادة 62 من القانون 18-07، يتمثل السلوك الاجرامي في هذه الجريمة في فعل الإفشاء، والذي يعرف بأنه: "الكشف عن واقعة لها صفة السر، ويصدر ممن علم بالسر لإطلاع الغير عليه وعلى الشخص الذي يتعلق به فهو نقل معلومات ولا يتحقق الإفشاء لمجرد نقل المعلومات وانما بتحديد الشخص الذي يتصل به"، ويستوي أن يكون الإفشاء شفهيًا أو مكتوبًا عاديًا أو إلكترونيا لأن المشرع الجزائري لم يحدد طبيعته، أو يكون علنيا أو غير علني كمن يبعث برسالة خاصة ورقية أو إلكترونية عن طريق الهاتف النقال أو مواقع التواصل الإجتماعي لغيره تحتوي على معطيات شخصية، كما يستوي أن يكون صريحا أو ضمنيا أو إفشاء كليًا للمعطيات أو جزئيًا[3]، من قِبل كل أعضاء السلطة الوطنية لحماية المعطيات الشخصية[4]،

---

[1] طباش عزالدين، المرجع السابق، ص 56.

[2] نبيلة رزاقي، المرجع السابق، ص 2006.

[3] بهاء المري، المرجع السابق، ص597- 598.

[4] المادة 23 من القانون 18-07 تنص على أنه " تتشكل السلطة الوطنية من:

- ثلاث (3) شخصيات، من بينهم الرئيس، يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عمل السلطة الوطنية،

والأمين التنفيذي ومستخدمو الأمانة التنفيذية الذين ألزمهم هذا القانون بالحفاظ على سرية أي معلومة يطلعون عليها خلال ممارسة مهامهم أو بمناسبة ممارستها[1]، ومثال هذه الجريمة المعطيات الطبية مثلا المسجلة بغرض الاستفادة من التأمين أو لغرض أبحاث طبية ثم يقوم من يسيطر على نظام المعالجة الآلية للمعطيات بإفشاء المعطيات إلى جهة أخرى تقوم بأبحاث بخصوص مرض معين، وهذا الشخص الذي تم إفشاء المعطيات إليه لا علاقة له بالنظام المعلوماتي[2].

وهذه الجريمة عمدية، تتطلب توفر القصد الجنائي بعنصريه وهما: أن يعلم الجاني بأن المعطيات التي يعالجها هي معطيات شخصية[3]، وأنها تدخل ضمن الأسرار المهنية[4]، وعلمه

- ثلاثة (3) قضاة، يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة،
- عضو من كل غرفة من البرلمان يتم اختياره من قبل رئيس كل غرفة، بعد التشاور مع رؤساء المجموعات البرلمانية،
- ممثل (1) عن المجلس الوطني لحقوق الانسان،
- ممثل (1) عن وزير الدفاع الوطني،
- ممثل (1) عن وزير الشؤون الخارجية،
- ممثل (1) عن الوزير المكلف بالداخلية،
- ممثل (1) عن وزير العدل حافظ الأختام،
- ممثل (1) عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيات والرقمنة،
- ممثل (1) عن الوزير المكلف بالصحة،
- ممثل (1) عن وزير العمل والتشغيل والضمان الاجتماعي،

يتم اختيار أعضاء السلطة الوطنية، حسب اختصاصهم القانوني و/ أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي.

يمكن السلطة أن تستعين بأي شخص مؤهل، من شأنه مساعدتها في أشغالها.

يعين رئيس وأعضاء السلطة الوطنية، بموجب مرسوم رئاسي، لعهدة مدتها خمس (5) سنوات قابلة للتجديد. "

[1] أنظر المادة 27 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] علي نعمة جواد الزرفي، المرجع السابق، ص109 - 110.

[3] خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية دراسة مقارنة، د.ط، دار الكتب والدراسات العربية، د. ب. ن، 202، ص79.

[4] مليايني عبد الوهاب، المرجع السابق، ص385.

أنه يفشي هذه المعطيات لشخص لا يجوز له قانون معرفتها والعلم بها، إضافة إلى أنه يجب أن تتجه إرادته إلى ارتكاب فعل الإفشاء أيا كانت صورته أو وسيلته.[1]

د_ جريمة الإعتداء على حقوق الشخص المعني: يقوم الركن المادي في هذه الجريمة عند رفض المسؤول عن المعالجة حقوق الشخص المعني صاحب المعطيات المزمع معالجتها، وهذه الحقوق تتمثل في حقه في الإعلام أو الولوج أو التصحيح أو الإعتراض التي خولها المشرع له، بغرض ممارسته رقابة على معطياته الشخصية الخاضعة للمعالجة[2]، في مواجهة المسؤول عن المعالجة، لحماية حياته الخاصة، حيث جرم كل إعتداء على هذه الحقوق بموجب القانون 18-07[3]. وهذه الجريمة جريمة عمدية، تمثل صورة الركن المعنوي لها في القصد الجنائي بعنصريه العلم والإرادة، حيث يكون المسؤول على المعالجة على علم بأنه يرفض منح الشخص المعني حقوقه التي نص عليها المشرع بموجب القانون 18-07، وتتجه إرادته إلى إرتكاب هذا الفعل المُجَرم.

هـ_ جريمة عدم مراعاة أحكام نقل معطيات نحو دولة أجنبية: يعتبر انتقال المعطيات، أو تبادلها من أهم الحركات التي تتميز بها المعطيات في الفضاء السيبراني، وعلى شبكة الانترنت، حيث تنتقل بين الشبكات بأنواعها، والتطبيقات، وقواعد المعطيات، والخدمات، وغيرها من الأجهزة والبرامج التي تقوم بمعالجتها[4].

---

[1] خالد حسن أحمد، المرجع السابق، ص79.

[2] مشتة نسرين، بن عبيد إخلاص، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد بن يحي الونشريسي، تيسمسيلت، الجزائر، المجلد 06، العدد 01، 2021، ص 684.

[3] كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية لقانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد 2 ، ديسمبر 2020، ص 63.

[4] باسم محمد فاضل مدبولي، المرجع السابق، ص 80.

نصت على هذه الجريمة المادة 67 من القانون 18-07، حيث السلوك الاجرامي فيها يتمثل في نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادة 44 من نفس القانون السابق ذكره، دون الحصول على ترخيص لنقلها من السلطة الوطنية، وكذلك في حالة عدم كفاية ضمانات الحماية التي ستوفرها الدولة التي ستحال اليها المعطيات الشخصية، أو إحالة معطيات إلى دولة أخرى وفي هذا التحويل مساس بالأمن العمومي والمصالح الحيوية[1]، وتعتبر هذه الجريمة عمدية تتطلب العلم والإرادة.

و_ جريمة مخالفة الإجراءات التنظيمية والتقنية لسلامة المعطيات: أو كما أطلق عليها المشرع تسمية جريمة خرق المسؤول عن المعالجة للإلتزامات المنصوص عليها في المادة 38 و39 من القانون 18-07، حيث يصعب في هذه الجريمة تحديد الركن المادي تحديدًا دقيقًا، كونها تتطلب سلوك إجرامي إيجابي ذو طبيعة مختلفة، وهو سلوك وقائي يهدف إلى حماية سلامة المعطيات الشخصية، هذا ما أكدته العبارات الفضفاضة التي استعملها المشرع في المادة 38 من القانون 18-07 كعبارة "التدابير التقنية والتنظيمية الملائمة" وعبارة "مستوى ملائما من السلامة"[2]، حيث ألزم المسؤول عن المعالجة باتخاذ جملة من التدابير التقنية والتنظيمية، لكنه لم يقوم بتحديدها بدقة، وهذا فيه تعارض مع مبدأ الشرعية[3] الذي يفرض تحديد التجريم والعقاب، أما في هذه الحالة التي لم يتم فيها التحديد فقد يتخذ المسؤول عن المعالجة مختلف التدابير ولكن لسبب أو لأخر تقع الجريمة المتعلقة بالتلف أو الضياع أو النشر أو الولوج غير المشروع[4]، ووردت الإلتزامات التي نص عليها القانون 18-07 في

---

[1] أنظر المادة 44 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] بطيحي نسمة، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، كتاب جماعي خاص بالملتقى الدولي المحكم الخصوصية في مجتمع المعلومات، طرابلس بين 19- 20 /07/ 2019، مركز جيل البحث، العام السابع، العدد 26، لبنان، يوليو 2019، ص78 – 79.

[3] نصت عليه المادة 1 من ق.ع . ج " لا جريمة ولا عقوبة أو تدابير أمن بغير قانون".

[4] هشام بخوش، المرجع السابق، ص 232.

المادتين 38 و39 المتعلقة بمهام المسؤول عن المعالجة على سبيل الإلزام وهذا ما يعبر عنه مصطلح "يجب" الواردة فيهما[1]، ونص المادة 65 من نفس القانون أكد ما سبق ذكره من خلال معاقبة المسؤول عن المعالجة في حالة خرقه للإلتزامات السالفة الذكر، وبالتالي فهذه الجريمة جريمة عمدية تتوافر على العلم والإرادة، لا تقع عن طريق الخطأ[2].

ز_ جريمة تسهيل الاستعمال التعسفي أو التدليسي للمعطيات الشخصية: نصت عليها المادة 69 من القانون 18-07، ويقوم السلوك الإجرامي في هذه الجريمة عندما تُرتكب من طرف أشخاص محددون (المسؤول عن المعالجة، المعالج من الباطن، أو الشخص المكلف بالمعالجة)، والذي يتسبب في الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو تسهيل ذلك الاهمال[3]. **و**تتطلب هذه الجريمة قصدا جنائيا فيعلم الجاني أن الأفعال التي يقوم بها تسبب أو تسهل الاستعمال التعسفي للمعطيات ذات الطابع الشخصي المعالجة أو المستلمة، وإتجاه إرادته إلى القيام بهذه الجريمة، ويمكن أيضا ارتكابها عن طريق الخطأ في صورة الإهمال مثلا، ويمكن أن يكون الخطأ في أي صورة من صوره كعدم التبصر[4].

[1] أنظر المادة 38 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بنصها "يجب على المسؤول وضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي...".

وكذلك في المادة 39 من نفس القانون التي تنص على أنه " عندما تجرى المعالجة لحساب المسؤول عن المعالجة، يجب على هذا الأخير إختيار يقدم الضمانات الكافية المتعلقة بإجراءات السلامة التقنية والتنظيمية للمعالجات الواجب القيام بها ويسهر على إحترامها..."

[2] بخوش هشام، المرجع السابق، ص232.

[3] سليم محمد سليم حسين، المرجع السابق، ص155- 156.

[4] سليم محمد سليم حسين، المرجع نفسه، ص156.

ثانيا: الجرائم الماسة بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

1_ جريمة امتناع مقدم الخدمة عن إعلام السلطة الوطنية والشخص المعني عن إنتهاك المعطيات الشخصية :

نصت عليها المادة 66 من القانون 18-07، ويعتبر السلوك الإجرامي هنا سلوكًا سلبيًا وليس إيجابيًا، ويتمثل في عدم قيام مقدم الخدمة بإلتزام فرضه عليه القانون من خلال إمتناعه عن إعلام السلطة الوطنية والشخص المعني عن كل الانتهاكات الماسة بالمعطيات الشخصية[1]، والتي تتمثل في ضياع المعطيات الشخصية أو إفشائها أو الولوج غير المرخص به، مما يؤدي إلى المساس بالحياة الخاصة لصاحب هذه المعطيات[2]. وحسب نص المادة المذكورة أعلاه فإن هذه الجريمة عمدية تتطلب توفر القصد الجنائي العام فقط بعنصريه.

2_ جريمة الولوج غير المؤهل للسجل الوطني:

نصت عليها المادة 63 من القانون 18-07، ويتمثل السلوك المادي في ولوج غير المؤهلين للسجل الوطني، وغير المؤهلين هم كل شخص لم يرد إسمه في التصريح[3]، وإطلاعهم على السجل الوطني لحماية المعطيات الشخصية الذي تمسكه السلطة الوطنية[4].

---

[1] أنظر المادة 66 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 43 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] بن يوسف القينعي، المرجع السابق، ص 508- 509.

[4] المادة 28 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي تنص على أنه: " ينشأ سجل وطني لحماية المعطيات ذات الطابع الشخصي، يمسك من طرف السلطة الوطنية، وتقيد فيه:

- الملفات التي تكون السلطة
- العمومية مسؤولة عن معالجتها،
- الملفات التي يكون الخواص مسؤولين عن معالجتها،

وهذه الجريمة جريمة عمدية تتوفر على عنصر العلم بأن الشخص غير مؤهل للولوج إلى السجل الوطني لحماية المعطيات الشخصية، وإتجاه إرادته إلى إرتكاب فعل الولوج للسجل الوطني لحماية المعطيات الشخصية.

_ جريمة عرقلة عمل السلطات الوطنية:

نصت على هذه الجريمة المادة 61 من القانون السالف الذكر، ويتمثل الركن المادي فيها في ارتكاب أحد هذه الأفعال الإجرامية الثلاثة: الاعتراض على القيام بالتحقيق وإجراءاته، أو القيام بسلوك سلبي يتمثل في الإحجام عن تزويد أعضائها بالمعلومات والوثائق اللازمة لتنفيذ مهمتهم أو إخفاء أو حذف الوثائق أو المعلومات المذكورة، أو من خلال إرسال معلومات غير مختلفة عن الحقيقة وغير متطابقة مع مضمون التسجيلات أثناء تقديم هذا الطلب أو تقديمها بشكل غامض وغير واضح[1]، وهذه الجريمة عمدية، يتبين ذلك من طبيعة الأفعال التي تشكل الركن المادي، والتي لا تُرتكب عن طريق الخطأ، وإنما تتطلب القصد الجنائي لارتكابها، وذلك من خلال علمه بأن الأفعال التي يرتكبها تعتبر

- مراجع القوانين أو النصوص التنظيمية المنشورة المتضمنة إحداث ملفات عمومية،
- التصريحات المقدمة للسلطة الوطنية والتراخيص التي تسلمها،
- المعطيات المتعلقة بالملفات الضرورية للسماح للأشخاص المعنيين بممارسة حقوقهم المنصوص عليها في هذا القانون.

تعفى من التقييد في السجل الوطني الملفات التي يكون الغرض الوحيد من معالجتها مسك سجل موجه بموجب مقتضيات تشريعية أو تنظيمية، لإطلاع العموم.

غير أنه تدرج بالسجل المذكور، وجوبا، هوية، الشخص المسؤول عن المعالجة حتى يتمكن الأشخاص المعنيون من ممارسة الحقوق المنصوص عليها في هذا القانون.

تحدد شروط وكيفيات مسك السجل الوطني عن طريق التنظيم."

[1] أنظر المادة 61 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

عرقلة أمام ممارسة عمل السلطة الوطنية المنصوص عليها في المادة 61 من القانون 18-07[1]، وتتجه إرادته لارتكاب هذه الأفعال.

الفرع الثاني: العقوبات المقررة لقمع الجرائم الواقعة على المعطيات ذات الطابع الشخصي

على الرغم من نص القانون 18-07 على مختلف الآليات الإجرائية والمؤسساتية لحماية المعطيات ذات الطابع الشخصي، إلا أن غياب عنصر الإلزام فيها جعلها غير كافية لضمان حماية أكثر فعالية، لذا تم النص في هذا القانون على العقوبات الجزائية إضافة لما تم التطرق إليه[2]، بغرض تحقيق الردع بنوعيه العام والخاص.

لذا من خلال هذا الفرع سنتطرق إلى العقوبات الأصلية المقررة لكل من الشخص الطبيعي والمعنوي في المقام الأول، وإلى العقوبات التكميلية للشخص الطبيعي والمعنوي في المقام الثاني.

أولا: العقوبات الأصلية المقررة للشخص الطبيعي والمعنوي

1_ عقوبات الشخص الطبيعي:

ما يلاحظ على العقوبات الواردة في القانون 18-07 أنها عقوبات جُنحية كون جلها مدة الحبس فيها تتجاوز الشهرين، وتصل إلى 5 سنوات والغرامة فيها تتجاوز 20.000 دج. وهذا ما نصت عليها المادة 5 من قانون العقوبات[3]، وهذه العقوبات كما يلي:

[1] تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 04، العدد 02، السنة 2019، ص1547.

[2] كحلاوي عبد الهادي، بن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحي أحمد، النعامة، الجزائر، المجلد 07، العدد 02، 2021، ص 121.

[3] تنص المادة 5 من ق.ع.ج على أنه: " العقوبات الأصلية في مادة الجنح هي:

أ_ العقوبة التي تتراوح مدة الحبس فيها من سنة إلى 5 سنوات تكون في الجرائم التالية:

_ جريمة الاستعمال التعسفي أو التدليسي للمعطيات الشخصية حيث عاقبت المادة 69 من القانون 18-07 المسؤول عن المعالجة والمعالج من الباطن، وكل شخص مكلف بالنظر إلى مهامه بمعالجة المعطيات الشخصية إذا ارتكب هذه الجريمة بالحبس من سنة إلى5 سنوات وبغرامة من 100.000 دج إلى 500.000 دج[1].

_ جريمة عدم مراعاة أحكام نقل المعطيات ذات طابع شخصي نحو دولة أجنبية: عاقبت المادة 67 من القانون 18-07 بنفس عقوبة الحبس المقررة للجريمة السابقة إلا أنها تختلف عنها في قيمة الغرامة المالية حيث تتراوح قيمتها من 500.000 دج إلى 1.000.000دج.

ب_ العقوبة التي تتراوح مدة الحبس فيها من سنتين إلى 5 سنوات وبالغرامة من 200.000 دج إلى 500.000 دج تكون في الجرائم التالية:

_ جريمة معالجة المعطيات ذات الطابع الشخصي دون الحصول على التصريح أو الترخيص: يعاقب على هذه الجريمة بموجب المادة 56 من القانون 18-07 كما سبق وأن ذكرنا[2].

_ جريمة معالجة معطيات حساسة دون موافقة الشخص المعني: وفقا لنص المادة 57 من القانون 18-07 يعاقب على هذه الجريمة بنفس مدة الحبس والغرامة المقررة للجريمة السابقة[1].

---

1) الحبس مدة تتجاوز شهرين إلى خمس سنوات ماعدا الحالات التي يقرر فيها القانون حدود أخرى، الغرامة التي تتجاوز 20.000 دج ".

[1] أنظر المادة 69 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 56 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

_ جريمة السماح لغير الأشخاص المؤهلين بالولوج لمعطيات ذات طابع شخصي: ونصت على عقوبة هذه الجريمة المادة 60 من القانون 18-07 وهي نفس العقوبة السالفة الذكر بالنسبة لمدة الحبس وقيمة الغرامة المالية[2]

ج _ الجرائم التي مدة عقوبتها من سنة إلى 3 سنوات وغرامة من 100.000 دج إلى 300.000 دج:

_ جريمة الاعتداء على حقوق الشخص المعني: نصت على العقوبة المقررة لهذه الجريمة المادة 55 من القانون 18- 07[3].

_ جريمة الجمع والتخزين غير المشروع للمعطيات الشخصية: لها نفس عقوبة الجريمة السابقة، وفقا لنص م 59 من القانون 18-07[4].

_ جريمة امتناع مقدم الخدمة عن اعلام السلطة الوطنية والشخص المعني عن إنتهاك المعطيات الشخصية: ويعاقب عليها بالعقوبة السالفة الذكر، أو بالغرامة أو بالحبس فقط[5].

_ جريمة الولوج غير المؤهل للسجل الوطني: يعاقب على هذه الجريمة بنفس العقوبة[6].

---

[1] أنظر المادة 57 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 60 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 55 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] أنظر المادة 59 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] أنظر المادة 66 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[6] أنظر المادة 63 من من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

د_ الجرائم التي مدة الحبس فيها من ستة أشهر إلى 3 سنوات:

_ جريمة الاحتفاظ بالمعطيات الشخصية في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم وإدانات وتدابير أمن لها نفس عقوبة الحبس المذكورة أعلاه ويعاقب عليها بغرامة من 60.000 دج إلى 300.000 دج[1].

هـ_ الجرائم التي مدة عقوبتها من ستة أشهر إلى سنتين:

_ جريمة الإنحراف عن الأغراض أو الغايات من المعالجة الآلية للمعطيات الشخصية: يعاقب عليها بمدة الحبس المذكورة أعلاه، وبغرامة من 60.000 دج إلى 100.000 دج أو بإحدى هاتين العقوبتين فقط[2].

و_ الجرائم التي مدة عقوبتها من ستة أشهر إلى سنة:

_ وتتمثل في جريمة عرقلة عمل السلطة الوطنية المعاقب عليها عليها بموجب المادة 61 من القانون 18-07 بالعقوبة المذكورة أعلاه وبغرامة من 60.000 إلى 200.000 دج أو بإحدى هاتين العقوبتين فقط[3].

ز_ الجرائم التي عقوبتها تتراوح من شهرين إلى سنتين والغرامة من 20.000 دج إلى 200.000 دج: تتمثل في جريمة الإعتداء على حقوق الشخص المعني بمعالجة معطياته،

[1] أنظر المادة 68 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 58 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 61 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

والمتمثلة في الحقوق المنصوص عليها بموجب المواد 32 و34 و35 و36 من القانون 18-07[1].

ح_ العقوبة من شهر إلى 6 أشهر وغرامة من 20.000 إلى 100.000 دج[2] تكون في جريمة الإفشاء غير المشروع للمعطيات الشخصية وهي العقوبة التي نصت عليها المادة 301 من قانون العقوبات الجزائري[3].

ي- الجرائم التي عقوبتها الغرامة من 200.000 دج إلى 500.000 دج هي:

_ جريمة خرق المسؤول عن المعالجة الالتزامات المنصوص عليها في المادتين 38 و39 من القانون 18-07، وجريمة الإحتفاظ بالمعطيات الشخصية أكثر من المدة القانونية اللازمة المنصوص عليها في التشريع، أو بعد المدة التي وردت في التصريح أو الترخيص[4].

2_ عقوبات الشخص المعنوي:

تكون عقوبة الشخص المعنوي المرتكب لجنحة من الجنح المنصوص عليها في القانون 18-07، وفقا للقواعد المنصوص عليها في قانون العقوبات[5]، والمنصوص عليها بموجب المادة 18 مكرر والمتمثلة في الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على هذه الجريمة[6].

---

[1] أنظر المادة 64 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 301 من ق. ع. ج.

[3] أنظر المادة 62 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] أنظر المادة 65 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] أنظر المادة 70 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[6] أنظر المادة 18 مكرر من ق.ع.ج.

ويجب أن ننوه في هذا الصدد إلى أن العقوبة المقررة لمحاولة إرتكاب إحدى الجنح المنصوص عليها في القانون 18-07 حسب القواعد العامة المعروفة لدينا هي عدم المعاقبة على المحاولة في الجنح إلا بنص صريح هذا ما نصت عليه المادة 31 ق.ع.ج[1]، لذا تم النص بموجب المادة 73 من القانون 18-07 بأنه يعاقب على إرتكاب إحدى هذه الجنح المنصوص عليها في هذا القانون بنفس العقوبة المقررة للجريمة التامة[2].

وما يجدر بنا الإشارة إليه أن عود الشخص الطبيعي أو المعنوي يعتبر ظرف مشدد عند إرتكاب جنحة جديدة من الجنح المنصوص عليها بموجب القانون 18-07 بعد صدور حكم نهائي عن جريمة سابقة[3]، حيث تضاعف العقوبة المنصوص عليها لهذه الجريمة[4].

ثانيا: العقوبات التكميلية للشخص الطبيعي والمعنوي

نصت المادة 71 من القانون 18-07[5] أنه يمكن أن يتعرض الأشخاص الذين يخالفون هذا القانون إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات[6]،

---

[1] أنظر المادة 31 من ق.ع.ج.

[2] أنظر المادة 73 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أحسن بوسقيعة، المرجع السابق، ص 417.

[4] أنظر المادة 74 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[5] أنظر المادة 71 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[6] حيث نصت المادة 9 من ق.ع.ج على العقوبات التكميلية بالنسبة للشخص الطبيعي والمتمثلة في الحجر القانوني، الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية، تحديد الإقامة، المنع من الإقامة، المصادرة الجزئية للأموال، المنع المؤقت من ممارسة مهنة أو نشاط، إغلاق المؤسسة، الإقصاء من الصفقات العمومية، الحظر من إصدار الشيكات و/ أو استعمال بطاقات الدفع، تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة، سحب جواز السفر، ونشر أو تعليق حكم أو قرار الإدانة.

ونصت المادة 18 مكرر البند 2 على العقوبات التكميلية بالنسبة للشخص المعنوي في مواد الجنايات والجنح، والمادة 18 مكرر 1 في مواد المخالفات. أنظر المادة 18 مكرر والمادة 18 مكرر 1 من ق.ع.ح.

وما يلاحظ أن المشرع لم يحدد نوع الأشخاص في المادة 71 من القانون 19-07 السالفة الذكر، وبالتالي هو يقصد بعبارة الأشخاص الأشخاص الطبيعيين والمعنويين معا، وما يُستنتج من عبارة "يمكن" أن العقوبات التكميلية التي يتم تطبيقها على مخالف هذا القانون هي جوازية، وهذا هو الأصل أن تكون العقوبات التكميلية جوازية[1]، إضافة إلى ذلك نص القانون 18-07 على عقوبة تكميلية أخرى لم يتم النص عليها في قانون العقوبات والمتمثلة في الأمر بمسح كل أو جزء من المعطيات ذات الطابع الشخصي التي هي محل معالجة ونتج عنها إرتكاب الجريمة، والأشخاص المؤهلين لمعاينة مسح هذه المعطيات هم أعضاء ومستخدمو السلطة الوطنية[2].

وما يجدر بنا الإشارة إليه أنه نصت م 72 من القانون 18-07 بأنه يتم مصادرة محل الجريمة المتعلقة بالمعطيات الشخصية، لأجل إعادة تخصيصه أو تدميره، على نفقة المحكوم عليه[3].

[1] أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الرابعة عشر، دار هومه، 2014 ، ص 326.

[2] أنظر المادة 71 من القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 72 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

الفصل الثاني: السياسة الجنائية الوطنية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات على المستوى الإجرائي

إن إقرار حماية جنائية موضوعية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من خلال التجريم والعقاب الوارد في النصوص القانونية السابقة الذكر في الفصل الأول، غير كافٍ بل يتطلب تطبيق فعلي للقوانين الموضوعية بغية تفعليها، وتطبيق هذه النصوص لا يكون إلا من خلال الإجراءات التي تضمن ذلك والتي تعتبر آلية من آليات السياسة الجنائية.

لذا قام المشرع الجزائري باستكمال السياسة الموضوعية بسياسة إجرائية خاصة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وهذا نظرا لطبيعتها الخاصة التي محلها البيئة الرقمية، إستحدث بموجبها تدابير وإجراءات خاصة للوقاية ومنع وقوع هذه الجرائم تجسيدًا لسياسة جنائية وقائية تجابه الخطر قبل الضرر، وإن لم يتم منع وقوع هذه الجرائم فإنه يتم إتباع إجراءات لمكافحتها، لكن طبيعة هذه الجرائم الخاصة جعلت من القواعد الجزائية الإجرائية التقليدية غير كافية للبحث والتحري والتحقيق فيها لذا تم استحداث قواعد إجرائية خاصة بهذا النوع من الجرائم تشمل مرحلتي البحث والتحري والتحقيق، إضافة إلى إستحداثه لجهات قضائية ذات إختصاص موسع لأجل التصدي لهذا النوع من الجرائم المستحدث والمتطور.

لذا سيتم التعرض إلى مختلف الإجراءات الوقائية وإجراءات مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال تقسيم هذا الفصل الذي قسمناه إلى الإجراءات الوقائية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الأول)، القواعد الجزائية الإجرائية المستحدثة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المبحث الثاني).

المبحث الأول: الإجراءات الوقائية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تهتم غالبية الدول بمجال الوقاية والمنع من الجريمة، من خلال تدابير إجرائية إستباقية للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وهذه الوقاية ترتبط بالعديد من المجالات منها مجال الإعلام الذي له دور فعال في التثقيف حول هذه الجرائم وكيفيات الوقاية منها وتجنبها، خاصة من جانب الإعلام الأمني، ناهيك عن دور المجتمع المدني في التوعية والتحسيس بخطورة هذه الجرائم، وتعتبر الوقاية من محاور السياسة الجنائية الاستباقية، التي لا تقتصر فقط على السياسة الجنائية الاستباقية في المجال الموضوعي، وإنما تمتد لتشمل السياسة الإجرائية.

وتقوم الوقاية على عنصرين أساسيين يتمثلان في الوقاية العامة التي تتناول وضع الخطط والبرامج الشاملة من قبل السلطات والهيئات المختصة والتي من شأنها القضاء على العوامل المؤدية إلى الإجرام أو المهيأة له، وذلك قصد الكشف المبكر عنها، والوقاية الخاصة التي يعتمدها الأفراد بوسائلهم الخاصة من أجل الابتعاد عن الظروف التي يمكن أن تجعل منها هدفا للإعتداء عليهم[1]، وفي هذا المبحث ستقتصر الدراسة على الوقاية العامة دون الوقاية الخاصة[2] أو ما يطلق عليها الذاتية.

---

[1] محمد السعيد تركي، نسيغة فيصل، سياسة الوقاية والمنع من الجريمة، مجلة البحوث والدراسات، جامعة حمه لخضر، الوادي، الجزائر، المجلد 15، العدد01، شتاء 2018، ص244.

[2] وتكون الوقاية الخاصة الذاتية بعدة طُرق مثلا من خلال:

_ تفعيل المصادقة الثنائية على جميع الحسابات الشخصية كالفيس بوك، تويتر، حساب جوجل، البريد الالكتروني ومختلف الحسابات الالكترونية ومواقع التواصل الاجتماعي

_ استخدام كلمات مرور قوية: لأجل حماية أنظمة المعالجة الآلية للمعطيات وحماية المعطيات الشخصية، وذلك من خلال استخدام برامج مخصصة لإدارة كلمات المرور الجديد لكل الحسابات والأنظمة المعلوماتية، وهذه البرامج تذكر بتحديث كلمات المرور دوريا.

- ✓ وتكون كلمات المرور قوية من خلال استخدام كلمات مرور طويلة تتكون من حروف ورموز وأرقام.
- ✓ تجنب استخدام كلمات المرور نفسها في أكثر من نظام أو موقع أو حساب.
- ✓ تجنب مشاركة كلمة المرور.

والتي تتجسد من خلال اتباع الأساليب المستحدثة في السياسة الجنائية للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، وبروز دور السلطات (المؤسسات) الوقائي من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الثاني).

المطلب الأول: اتباع الأساليب المستحدثة للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

بغرض الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، لابد من اتباع الأساليب والآليات الوقائية المستحدثة في السياسة الجنائية، ويكون ذلك من خلال مسايرة متطلبات عملية الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (الفرع الأول)، وإستحداث إجراءات للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ملقاة على عاتق مقدمي الانترنت (الفرع الثاني).

✓ ضرورة تحديث كلمات المرور دوريا، مرة واحدة على الأقل في كل 6 أشهر.

_ استخدام برامج الحماية ضد الفيروسات (anti-virus protction) ومن الضروري تحديث كافة تعريفات الفيروسات والمحركات لأجل التأكد من فعالية برامج مكافحة الفيروسات.

_ سرعة الإبلاغ: خاصة إذا تم إختراق مواقع التواصل الاجتماعي يجب على المستخدم الابلاغ فورًا عن الاختراق الذي تعرض له ليقوم الموقع بإزالة هذا التعدي على وجه السرعة.

الفرع الأول: مسايرة متطلبات عملية الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تحتاج إلى تجهيز بشري وتقني ومراكز للوقاية.

تميز الإتجاه الحديث في السياسة الوقائية بالاهتمام المباشر بالجهاز البشري العامل في ميدان الوقاية من الجريمة انطلاقا من الحقيقة الأساسية التي تحكم النظام الوقائي، حيث يعتبر العنصر البشري أهم عنصر في العملية الوقائية، وذلك من خلال الاهتمام بالتأهيل والتدريب على العمليات التخطيطية والتنفيذية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات[1].

أولا: التجهيز للعملية الوقائية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

1_ التجهيز البشري لعملية الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

ويتم ذلك من خلال تدريب وتأهيل العناصر البشرية حول آليات الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وتعددت تعريفات التدريب من قِبل الأكاديميون والمتخصصون في هذا المجال، حيث عرفه البعض بأنه "عملية يكتسب فيها المتدرب المعارف والمهارات والاتجاهات، من خلال جهد منظم ومخطط، يهدف إلى تغيير سلوكه بشكل إيجابي، مما ينعكس على الارتقاء بمستوى أدائه في مجال عمله الحالي والمستقبلي"[2]، عرفه بعض الفقهاء: بأنه "عملية إنسانية مستمرة تبدأ لحظة إختيار الفرد للوظيفة وتستمر معه طول حياته الوظيفية لتأهيله وتنمية قدراته المعرفية والفنية"[3].

---

[1] محمد السعيد تركي، نسيغة فيصل، المرجع السابق، ص 246.

[2] محمد السيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، 2006، ص 609. مقال منشور على الرابط التالي:
https://down.ketabpedia.com/files/bkb/bkb-ab01080-ketabpedia.com.pdf

[3] محمد السيد عرفة، المرجع نفسه، ص611.

تعددت طرق وآليات التدريب على الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث يكون ذلك من خلال تأهيلهم تأهيل قانوني (نظري وتطبيقي)، وكذلك تأهيلهم تأهيل فني تقنين وتعليمهم الإجراءات الوقائية السابقة واللاحقة لارتكاب الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات[1]، فالتدريب يتطلب تكوينا متخصصا في مجال تقنيات تكنولوجيات الإعلام والإتصال وأنظمة المعالجة الآلية للمعطيات، وبكل ماله علاقة بالبيئة الرقمية لأن نقص هذا التكوين أو إنعدامه يشكل عائقا على الوقاية من هذه الجريمة وعلى الاستدلال والتحقيق بشأنها، فهذه العملية تتطلب التأهيل المناسب من الجهات المختصة، وإستقطاب الخبراء المختصين في هذا النوع من الجرائم للإشراف عليها، وتوفير المعدات المتطورة في هذا المجال[2]، وحتى تكون نتائج التدريب إيجابية يجب أن يتمتع المدرب بالكفاءة العلمية والقدرات الذهنية والنفسية لتلقي التدريب، وكما يضيف بعض الخبراء أنه يجب توفر الخبرة الكافية في المجالات المتعلقة بالعمليات التي ترد على الحاسوب والبرمجة، ويجب أن يشتمل البرنامج التدريبي التدريب أيضًا على طرق التوعية للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى آليات وإجراءات التدريب اللاحقة التي تكون بعد وقوع الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات[3]، ويتم كذلك التدريب من خلال استخدام المحاكاة الحاسوبية التي من خلالها يتم التعايش مع ظروف وملابسات واحتمالات ممكنة الوقوع في الواقع كالاعتداءات على أنظمة المعالجة الآلية للمعطيات من خلال أساليب جد متطورة والتعامل مع هذه الاعتداءات افتراضيا بأساليب

[1] ياسر محمد الكومي أبو الحطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف، الإسكندرية، 2014، ص63.

[2] عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، الجزائر، 2021، ص 124- 125.

[3] محمد نصر محمد، المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015، ص63.

تمكن المتدرب من القدرة على التعامل معها في الحياة العملية الواقعية والوقاية من حدوثها مستقبلا[1].

ويستهدف التدريب غالبا عناصر الأجهزة الأمنية التي تخضع **للتدريب الأمني** والذي يُعرف على أنه "كل ما يمكن الأجهزة والمؤسسات المعنية بالوقاية من الجرائم المستحدثة، من مواجهتها والتصدي لها بوعي عال وإدراك ناضج وقدرة عالية وكفاءة رفيعة المستوى، من خلال إعداد وتأهيل عناصرها وفقا لأحدث الأساليب وأدقها وبتقنيات تأهيلية متطورة تنسجم وتتقدم على الأساليب الجنائية وتفوقها في القدرة على منعها وكشفها وتشخيص مرتكبيها"[2]، فهذا النوع من التدريب يقلل من معدلات الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بكل أشكالها وأنواعها للحد الأدنى إذا تعذر منع وقوعها[3]، ويتطلب تدريب عناصر الأجهزة الأمنية، التحديث المستمر الذي يتماشى مع التطورات الحاصلة، وإتباع الأساليب العلمية، وتأهيل كوادرها، ولا سيما الشرطة العلمية، وكذلك استكمال المعدات التقنية والأجهزة العلمية الحديثة التي تحتاجها هذه العناصر، وتدريبهم على كيفيات استخدامها، بغرض تحقيق ما يضمن لها الأخذ بأحدث التطورات التكنولوجية[4]، التنبؤ قبل حدوث هذه الجرائم من خلال برمجيات الحاسب الوقائية التي تكتشف التهديدات السيبرانية مبكرًا.

[1] ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص- قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، 2015-2016، ص211.

[2] كمال بوبعاية، السعيد برابح، التدريب ودوره في مكافحة الجريمة المنظمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 6، العدد2، 2021، ص 142.

[3] عامر خضير حميد الكبيسي، التدريب الإداري والأمني رؤية معاصرة للقرن الحادي والعشرين، ط 1، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2010، ص 67.

[4] محمد السعيد تركي، نسيغة فيصل، المرجع السابق، ص240- 241.

وتعتبر الضبطية القضائية، مكلفة بالوقاية من الجريمة[1] وردعها وتطويقها، كون ضباط الشرطة القضائية يجمعون بين صفتي الضبط القضائي وصفة الضبط الإداري، فكل من عناصر الشرطة وعناصر الدرك الوطني مهما كانت رتبهم ودرجاتهم، يعتبرون ضباط شرطة إدارية ويخضعون لرؤسائهم الاداريين تحت وصاية وزارة الداخلية إذا كانوا من الأمن الوطني، أو تحت وصاية وزارة الدفاع إن كانوا من الدرك الوطني، ومهمتهم الوقاية من الجرائم، واتخاذ كافة الاحتياطات اللازمة لمنع وقوعها عن طريق إقرار الأمن والنظام داخل المجتمع[2]، هذا قبل حدوث الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ولهم دور وقائي كذلك بعد حدوثها من خلال منع تفاقمها وتوسع نطاقها ومن خلال محاصرتها خاصة إذا كانت الأنظمة المعلوماتية مرتبطة ببعضها البعض.

2_ التجهيز الفني والتقني لعملية الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

تتطلب الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تجهيزات فنية وتقنية، لتمكين العناصر البشرية المختصة بالوقاية من القيام بهمة الوقاية الاستباقية من هذه

[1] وما يجدر بنا الإشارة إليه أنه يوم 02 أوت 2022 تم توقيع مذكرة تعاون مشتركة بين كل من المديرية العامة للأمن الوطني وقيادة الدرك الوطني بغرض ترابط الجهود المبذولة من طرف كلا منهما، فتهدف هذه المذكرة إلى تدعيم الجهود للوقاية من الجرائم بمختلف أنواعها بما فيها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال وضع خطط مشتركة بينهما لأجل التكامل العملياتي، وهذه الاتفاقية تهدف إلى تعزيز التعاون التقني والعلمي بين هذين المؤسساتين الأمنيتين وتبادل المعلومات والخبرات وبرمجة دورات مشتركة لتدريب. أنظر المديرية العامة للأمن الوطني، الوثيقة منشورة على الرابط التالي:

https://www.algeriepolice.dz/IMG/pdf/com_ar_02.08.2022-2.pdf

تم الاطلاع عليه بتاريخ: 2023/04/01 على الساعة 20:00.

[2] علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الأول الاستدلال والاتهام، ط 3، دار هومه، الجزائر، د. س. ن ، ص16.

الجرائم[1]، ويكون التجهيز من خلال توفير التقنيات والبرامج التي تساعد على الوقاية من هذه الجرائم، واعتماد طرق تقنية للوقاية منها كتقنيات التشفير[2] مثلا وأمنية المعلومات.

ثانيا: إنشاء مراكز للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ومعاهد متخصصة في العلوم الجنائية

تعددت مراكز الوقاية من هذا النوع من الجرائم ومكافحتها، وسنتطرق إلى أهمها كمايلي:

1_مراكز الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ومكافحتها التابعة للدرك الوطني:

أ_ مركز البحث والتطوير: مركز البحث والتطوير للدرك الوطني (م.ب.ت–د.و) هو مؤسسة عسكرية ذات طبيعة علمية وتقني (EMST)، تم إنشاؤه سنة 2006، يتكون من دوائر ومختبرات ومكاتب الدعم التقني، حيث يهتم بالعديد من المجالات منها: الإجرام السيبراني والحركية، وتحليل المعطيات، وكذلك الأدلة الجنائية[3].

ب_ المركز الوطني لمكافحة الجريمة المعلوماتية: أنشأت قيادة الدرك الوطني المركز الوطني لمكافحة الجريمة الإلكترونية والذي لديه مهام وقائية وتتمثل أولها في المراقبة العامة للمضمون المعلوماتي: والتي هي مهام وحدة الحماية والتحليل (unité de veille et analyse) التي تسهر على تحليل المخزون المعلوماتي الخاصة بالاستعلامات على شبكة الانترنت

---

[1] محمد السعيد تركي، نسيغة فيصل، المرجع السابق، ص 246.

[2] **التشفير** هو: إخفاء المعطيات، بأساليب تجعل معناها يكون غير واضح ومفهوم للأشخاص غير المصرح لهم بالاطلاع عليها، فالتشفير يجعل الأشخاص غير المصرح لهم بالدخول يصلون للمعطيات الرقمية بشكل عادي لكنه يضمن أن يكون مضمون الملف المشفر غير مفوم لهم. للتفصل أكثر أنظر: باسم محمد فاضل مدبولي، المرجع السابق، ص26.

[3] الموقع الرسمي لقيادة الدرك الوطني، متوفر على الرابط التالي:
https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/crd/crd_ar.php
تم الإطلاع عليه بتاريخ 14 أفريل 2023 على الساعة 11:55.

وحماية بنوك المعلومات المفتوحة عبر الانترنت، أما الثانية تتمثل في الوقاية وهي مهام خلية المساعدة ومعالجة الحوادث المعلوماتية « Cellule d'assistance et de réponse aux incidents informatique » والوقاية منها حيث تسهر على حماية المواطنين وتقديم المساعدة لهم لأجل تخطي الجرائم الالكترونية على مستوى المؤسسات والمرافق الحكومية التابعة للدولة، وما يجدر بنا الإشارة إليه كذلك أن لها مهام ردعية تقوم بها الوحدة المركزية للتنسيق والتعاون «Unité centrale de coordination et de lutte contre la cybercriminalité » وتتفرع عنها على المستوى الولائي تتمثل في المحلية لمحاربة الجريمة الالكترونية[1].

ج ـ مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني: أنشئ في سنة 2008، يقع مقره في بئر مراد رايس[2]، وهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والإستعمال لقيادة الدرك الوطني، يعتبر نقطة محورية وطنية في مجال دعم أعمال الوقاية من الجرائم المعلوماتية والبحث عنها والتحقيق فيها، له مهام عديده، لاسيما تلك المتعلقة بالوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، فيقوم بمراقبة الاتصالات الإلكترونية لصالح الجهات القضائية ووحدات الدرك الوطني، وكذلك المراقبة بشكل متواصل والدائمة على شبكات الانترنت، وله كذلك مهام بعد ارتكاب الجريمة يقوم بإجراءات البحث والتحري والتحقيق عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في البيئة الرقمية بالتعاون مع مصالح الأمن والسلطات المختصة من خلال تقديم المساعدة

[1] حايطي فاطيمة، إجراءات التحقيق في الجرائم الإلكترونية (دراسة مقارنة)، أطروحة لنيل شهادة دكتوراه الطور الثالث، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، الجزائر، 2022-2023، ص122- 123.

[2] بارة سمير الأمن السيبراني(Cyper Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1 الحاج لخضر، باتنة، الجزائر، العدد 4، جويلية 2017، ص270.

عند إجراء المعاينة الالكترونية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والبحث عن الأدلة الرقمية، والقيام بعمليات التسرب الالكتروني[1].

د_ إنشاء معاهد متخصصة في العلوم الجنائية وعلم الإجرام:

_ المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني: نصت المادة 1[2] من المرسوم الرئاسي رقم 04-183 على إحداث هذا المعهد، موضوع تحت وصاية وزير الدفاع الوطني[3]، حيث يعتبر هذا المعهد داعم لقدرات الدرك الوطني في مكافحة الجريمة بجميع أشكالها وذلك بإدراج العلوم في العدالة الجنائية، كم أن التحكم في التقنيات الحديثة من شأنه أن يدعم قدرات المؤسسة لمكافحة الإجرام المتطور باستمرار والذي يعتمد على التكنولوجيات الجديدة[4].

---

[1] ربيعي حسين، المرجع السابق، ص185.

[2] المادة 1 من المرسوم الرئاسي رقم 04- 183 مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج عدد 41 مؤرخة في 9 جمادى الأولى عام 1425 الموافق 27 يونيو 2004.

[3] المادة 2 من نفس المرسوم الرئاسي المذكور أعلاه تنص "المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والإستقلال المالي.

ويوضع تحت وصاية وزير الدفاع الوطن.

ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، وبهذه الصفة، فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية".

وأنظر المادة: المادة 3 من نفس المرسوم الرئاسي تنص: " يكون مقر المعهد بمدينة الجزائر، ويمكن نقله إلى أي مكان أخر من التراب الوطني بقرار من وزير الدفاع الوطني.

يمكن إحداث ملحقات، عند الحاجة، بقرار من وزير الدفاع الوطني."

[4] الموقع الرسمي لقيادة الدرك الوطني، متوفر على الرابط التالي:

https://www.mdn.dz/site_cgn/sommaire/presentation/unit_spe/incc/incc_ar.php

تم الإطلاع عليه بتاريخ 07 أفريل 2023 على الساعة 10:18.

له مهام وقائية متعددة أهمها: مشاركته في الدراسات والبحوث وكذلك التحاليل المتعلقة بالوقاية والتقليل من جميع أشكال الإجرام[1]، بما فيها الإجرام المستحدث والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ويساهم في ضبط وتحديد سياسة جنائية مثلى لمكافحة الإجرام[2] بكل أشكاله، وتتضمن هذه السياسة كذلك السياسة الوقائية لمكافحة مختلف أشكال الإجرام بما فيه الإجرام المتعلق بأنظمة المعالجة الآلية للمعطيات، ويقوم بإجراء البحوث المتعلقة بهذه الجرائم وإنجازها باستخدام تقنيات التكنولوجيا دقيقة، يشارك في الملتقيات والمحاضرات والندوات الوطنية والدولية لتطوير مستخدمي المعهد، ويشارك في تنظيم دورات تحسين المستوى والتكوين في تخصصات العلوم الجنائية[3] ويضع تصور للأبحاث الموكلة إلى الغير ويضمن مراقبتها وتقديرها[4].

يقوم بإجراء البحوث المتعلقة بهذه الجرائم وإنجازها باستخدام تقنيات دقيقة، ويشارك في المنتديات والمؤتمرات والندوات الوطنية والدولية لتطوير مستخدمي المعهد، ويشارك في تنظيم دورات لتحسين المستوى والتدريب بعد التخرج في تخصصات العلوم الجنائية ويضع تصورًا للبحث الموكل إلى الآخرين ويضمن مراقبتها وتقييمها.

ويجدر بنا الاشارة في هذا الصدد إلى أنه يقوم كذلك بالعديد من المهام التي تتعلق بالتحري والتحقيق من خلال توفير الدعم التقني في مرحلة القيام بالتحريات المعقدة والمتشعبة باستخدام المناهج العلمية والتقنية، وإنجاز الخبرات العلمية بناء على طلبات

[1] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

[2] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

[3] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

[4] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

القضاة والمحققين والسلطات المؤهلة، لإقامة الأدلة التي تتيح التعرف على مرتكبي الجرائم[1]، إضافة إلى تصميم بنوك معطيات وإنجازها وفقا للقانون، ليستخدمها المحققون والقضاة بهدف استخراج الروابط الممكنة بين المجرمين وأساليب النشاط الإجرامي، والعمل على تعزيز وترقية البحوث التطبيقية وأساليب التحريات التي تثبت نجاعتها في مجال علم الإجرام والأدلة الجنائية على المستويين الدولي والوطني[2].

2_ المصلحة المركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التابعة للمديرية العامة للأمن الوطني:

أنشئتها المديرية العامة للأمن الوطني في جانفي 2015، تقوم بالعديد من الجهود العديد من الجهود الاستباقية من خلال النشاطات الوقائية والردعية، إضافة إلى ادراجها لبرامج متخصصة تدربية لعناصر الشرطة، في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وبرمجة دورات تكوينية وتربصات[3]، وقيامها باتخاذ تدابير استباقية للتصدي لهذه الجرائم عن طريق التوعية بخطورتها[4].

وتجدر بنا الإشارة إلى أن المديرية العامة للأمن الوطني تقوم بعمليات وقائية، تتخذها الجهات المختصة في مكافحة الاجرام المعلوماتي، وفرقها العملياتية التي تتبع الشرطة القضائية، من خلال اتخاذ مجموعة من التدابير الوقائية أهمها: تعزيز الأنشطة المرتبطة بالمنع المباشر من قبل أجهزة الشرطة المختصة في مجال مكافحة الجرائم السيبرانية، وأمن

[1] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

[2] أنظر المادة 4 من المرسوم الرئاسي رقم 04- 183 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي.

[3] حسين جيجة، سحواد نسيمة، جهود استباقية للأمن الوطني لتحقيق الأمن المعلوماتي والامتياز في الأداء، المديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015، ص141- 143.

[4] حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بتاريخ 16-17 نوفمبر، جامعة بسكرة، الجزائر، ص9.

وحماية أنظمة المعالجة الآلية لمعطيات والفضاء السيبراني الوطني، وممارسة اليقظة المعلوماتية، وكذلك البحث على الشبكات المفتوحة والبحث عن أي محتوى يشكل جنوحًا إلكترونيًا محظورًا قانونًا[1].

الفرع الثاني: استحداث إجراءات وقائية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ملقاة على عاتق مقدمي الخدمات

عرف المشرع الجزائري مقدمو الخدمات في المادة الثانية من القانون 09-04 على أنهم "1- أي كيان عام أو خاص يقدم لمستعملي خدماته، القدرة على الإتصال بواسطة منظومة معلوماتية و/ أو نظام للإتصالات،

2- وأي كيان أخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها"[2]، والجدير بالذكر هنا أن المشرع الجزائري لم يبين أنواعهم وأطلق عليهم تسمية واحدة وهي مقدمو الخدمات، لأنهم يشتركون جميعًا في نفس المسؤولية الجزائية إذا ما خالفوا القانون والالتزامات إذا ما قاموا بتقصير. وهذا خلافا للمشرع الفرنسي الذي عند تعريفه لمقدمي الخدمات، قسمهم إلى ثلاثة أنواع وعرف كل نوع منهم، وتمثلوا في: مقدمي (متعهدي خدمة التوصيل)، متعهدي الإيواء، مقدمي المضمون[3].

ولمقدمي خدمة الانترنت مهام وقائية تتمثل في مراقبة ومتابعة إستخدام وسائل تقنية الاتصالات الحديث كرسها المشرع من خلال الالتزامات المفروضة عليهم والتي تتمثل في:

[1] نعمان كريمة، الشرطة الجزائرية تتصدى لصناع الكراهية عبر المنصات الرقمية، مجلة إعلامية أمنية، تصدر عن المديرية العامة للأمن الوطني، العدد 149، أكتوبر 2021، ص32- 33.

[2] أنظر المادة 02 من من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي تبسة، الجزائر، 2017/ 2018، ص 141- 142.

أولا: الإلتزامات الوقائية لجميع مقدمي الخدمات

رتب المشرع الجزائري لمقدمي الخدمات التزامات تتمثل في:

أ_ مساعدة السلطات: ألزمت المادة 10 من القانون 09-04، مقدمي خدمة الانترنت بتقديم المساعدة للسلطات القضائية المختصة بالتحريات القضائية، بغرض جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها[1]، فيعتبر مقدم الخدمة له دورًا إيجابيا يتجلى بمساعدتهم للسلطة القضائية، في كشف المجرمين المعلوماتيين المرتكبين للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات[2]، وهذا يعتبر إجراء تسخير من قبل السلطة القضائية، والمشرع الجزائري لم يحدد نوع هذه الاتصالات، وبالتالي فهو يتعلق بجميع أنواع الاتصال أي كان شكلها، مكالمات هاتفية بنوعيها صوتية عن طريق الهاتف أو مواقع التواصل الإجتماعي بمختلف أنواعها أو مكالمات فيديو، أو إذا كانت في شكل رسائل عبر البريد الإلكتروني Email، أو رسالة نصية قصيرة SMS[3]، أو كانت على شكل رسالة MMS (Multimedia Messaging Service)[4] خدمة رسائل الوسائط المتعددة[5].

---

[1] أنظر المادة 10 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، مجلة دائرة البحوث القانونية والسياسية– مخبر المؤسسات الدستورية والنظم السياسية، العدد 4، جانفي 2018، ص 51.

[3] خدمة الرسالة القصيرة أو رُسَيلة (SMS) وهي اختصار لعبارة Short message service، موسوعة ويكيبيديا، متوفر على الرابط التالي:
https://ar.wikipedia.org/wiki/%D8%AE%D8%AF%D9%85%D8%A9_%D8%A7%D9%84%D8%B1%D8%B3%D8%A7%D9%84%D8%A9_%D8%A7%D9%84%D9%82%D8%B5%D9%8A%D8%B1%D8%A9 تم الاطلاع عليه بتاريخ 19/03/ 2022 على الساعة 18:00.

[4] أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2013/2012 ، ص 101.

[5] MMS (Multimedia Messaging Service) خدمة رسائل الوسائط المتعددة : تسمح بإرسال رسائل تحتوي على عناصر وسائط متعددة صوت، صورة، نص أغنية). موسوعة ويكيبيديا، متوفر على الرابط التالي:
https://ar.wikipedia.org/wiki/%D8%AE%D8%AF%D9%85%D8%A9_%D8%B1%D8%B3%D8%A7%D8%A6

ب_ حفظ المعطيات المتعلقة بحركة السير: ونصت كذلك نفس المادة السالفة الذكر عن إلتزام أخر لمقدمي الخدمات يتمثل في وضع المعطيات التي يتعين على مقدمي الخدمات حفظها تحت تصرف السلطات المكلفة بالتحريات القضائية، وحفظها ويكون ذلك وفقا للمادة 11 من نفس القانون[1]، وحددت نفس المادة السابقة مدة حفظ المعطيات سنة تُحسب من تاريخ تسجيل هذه المعطيات[2].

ج_ الالتزام بالسرية والشفافية: وذلك بهدف حماية الحياة الخاصة لمشتركي الانترنت، وتتمثل في: الحفاظ على معلومات مشترك خدمة الانترنت، وعدم الإدلاء بمعلومات المشتركين إلا إذا نص القانون على ذلك، ويترتب على خرق هذا الإلتزام تطبيق عليهم العقوبات المقررة في حالة إفشاء أسرار التحري والتحقيق[3].

%D9%84_%D8%A7%D9%84%D9%88%D8%B3%D8%A7%D8%A6%D8%B7_%D8%A7%D9%84%D9%85%D8%AA%D8%B9%D8%AF%D8%AF%D8%A9 تم الاطلاع عليه بتاريخ 03/19/ 2022 على الساعة 18:03.

[1] المادة 11 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال. تنص على أنه " مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدموا الخدمات بحفظ:

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال،

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة أو مقدميها،

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها."

[2] أنظر المادة 11 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[3] وسيمة مصطفى هنشور، النظام القانوني لمقدمي خدمات الإنترنت في التشريع الجزائري، مجلة البحوث القانونية والسياسية، العدد 5، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر، ديسمبر 2015، ص135.

ثانيا: الالتزامات الوقائية الخاصة بمقدمي خدمة الانترنت

نصت على هذه الإلتزامات المادة 12 من القانون 09-04، حيث أنه إضافة إلى الإلتزامات العامة المفروضة على مقدمي الخدمات، يقوم مقدمي خدمة الانترنت ب:

أ_ إلتزام مقدمي خدمة الأنترنت بسحب المحتوى غير المشروع: فعند علم مقدم الخدمة بطريقة مباشرة أم غير مباشرة بعدم مشروعية المحتوى أو مخالفته للقانون يسحبه فورا دون تمهل وبإستعجال أو يخزنها حتى تصبح غير ظاهرة للعيان ويحجبها عنهم ويمنع الدخول إليها من خلال غلق الموقع نهائيا أو تجميد الدخول إليه[1].

ويُلاحظ أنه لم يحدد المشرع الجزائري الحالات التي يكون فيها هذا المحتوى مخالف للقانون وغير مشروع أي مخالف للنظام العام والآداب العامة، وكما نعلم أن هذه العبارات فضفاضة تختلف من دولة إلى أخرى.

ب_ إلتزام مقدمي خدمة الأنترنت بوضع الترتيبات التقنية لحصر إمكانية الدخول للمعلومات غير المشروعة: هذا الإلتزام نصت عليه المادة 12 في فقرتها الأخيرة (ب)[2]، حيث من خلال هذه الفقرة يتضح أن المشرع الجزائري أشرك مقدمي خدمة الانترنت في التجكم إستخدام الانترنت وضبط ذلك، وجعله ملتزما بالقانون، من خلال دوره الفعال في تحديد الوصول للمحتوى غير المشروع والمخالف للنظام العام والآداب العامة، فبمجرد علمهم بوجود هذا المحتوى، يجب عليهم فورًا إعلام السلطات المختصة بجميع التفاصيل التي وصلت إلى علمهم[3].

[1] أنظر المادة 12 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] أنظر المادة 12 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] بن عزة محمد حمزة، المسؤولية القانونية لمتعاملي الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، الجزائر، 2018/ 2019، ص 208.

يتعين على مقدمي خدمة الانترنت اتخاذ كل التدابير والاجراءات اللازمة لضمان الحماية الدائمة لمحتوى الموزعات المفتوحة لمشتركيهم، حتى كون آمنة، وذلك لمنع الوصول لمحتوياتها إذا كانت مضامينها مخالفة للنظام العام والآداب العامة[1].

المطلب الثاني: دور السلطات الوقائي من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

التطور التكنولوجي وظهور الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، أدى إلى ظهور نوع جديد من الضبط يُطلق عليه الضبط الإداري الإلكتروني، تمارس هذا النوع من الضبط سلطات إستحدثها المشرع الجزائري، وهذه السلطات يغلب عليها الدور الوقائي بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بمختلف أشكالها سواء تلك الواقعة على النظام في حد ذاته، وإما التي تُرتكب بواسطته أم التي تقع على معطياته بشتى صورها، ولهذه السلطات دور لا يستهان به في مجال الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من خلال التدابير الإجرائية التي تقوم به ومثالها: إجراء الرقابة و تطبيقها لإجراءات التقييد كالترخيص والإذن التي تعتبر كذلك أساليب رقابية ومراقبة شبكات الانترنت وشبكات الاتصال والقيام بإجراء الحجب الالكتروني...الخ، وتتمثل هذه السلطات في سلطات الضبط الإداري (الفرع الأول)، و السلطات الادارية المستقلة (الفرع الثاني).

الفرع الأول: سلطات الضبط الإداري

لسلطات الضبط الإداري دور لا يستهان به في الوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، يتجلى من خلال الرقابة، التي تمارسها هذه السلطات والتي سنتطرق لها كما يلي:

[1] وسيمة مصطفى هنشور ، المرجع السابق، ص 135.

أولا: سلطة ضبط البريد والاتصالات الإلكترونية

تم إنشاء سلطة ضبط البريد والاتصالات الإلكترونية بموجب المادة 11 من القانون رقم 18-04، لهذه السلطة دور رقابي يتجلى من خلال نص المادة 13 من القانون 18-04 التي ورد فيها النص على نشاطها المدرج ضمن تقاريرها السنوية المحررة بشكل مستمر[1].

حيث تمارس دورها الرقابي من خلال مراقبة أنشطة المتعاملين معها وإجراء التحريات اللازمة لضبط ومنع وقوع المخالفات، وهذا يعني أن حريات وأنشطة المتعاملين في هذا القطاع ليست مطلقة وإنما مقيدة بالقانون، من خلال عملية الرقابة يُتَجنب إهدار المصالح المحمية، بعد منح التراخيص للمتعاملين الذين يستوفون الشروط المقررة، وتكون هذه الرقابة على شكل العديد من الصور[2] أهمها: حجب الشبكات والمواقع الإلكترونية كإجراء وقائي: وهو من الإجراءات الوقائية التي تمنع تنفيذ النشاط من قبل الجهة الرقابية المتمثلة في سلطة الضبط، حيث بموجبه تمنع المستخدمين من الوصول إلى مواقع أو شبكات اتصال معينة بشكل دائم أو مؤقت من أجل حماية النظام العام بعناصره المختلفة، مثل حجب المواقع الإباحية أو التي تروج للإرهاب بغرض التجنيد أو التمويل... الخ ، وما يجدر الإشارة إليه هنا أن نظام الحجب يتخذ شكلين: **الحجب الكلي**[3]، وذلك يكون من خلال التقييد الدائم وبصفة مستمرة للوصول إلى موقع ويب واحد أو أكثر، أو **الحجب الجزئي**[4] الذي يتمثل في

[1] رضا بو الجدري، وردة سالمي، سلطة ضبط البريد والاتصالات الالكترونية قراءة في المهام والصلاحيات من خلال أحكام القانون 18-04، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، الجزائر، المجلد 34، العدد 1، جامعة الإخوة منتوري قسنطينة 1، الجزائر، 2023، ص193.

[2] حايطي فاطيمة، المرجع السابق، ص43.

[3] مثال عن الحجب الكلي لمواقع الشبكات الإجتماعية: غلق مواقع التواصل الإجتماعي فايسبوك، تويتر، يوتيوب، إضافة إلى محرك بحث قوقل Google. للتفصيل أكثر أنظر: بلخير محمد آيت عويدة، الضبط الإداري للشبكات الإجتماعية الإلكترونية، أطروحة مقدمة لنيل دكتوراه علوم في الحقوق، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2019/2018، ص278.

[4] مثال عن الحجب المؤقت لمجموعة من مواقع الشبكات الاجتماعية الإلكترونية منها: فايسبوك وتويتر خلال شهر جوان 2016 وذلك بهدف منع تكرار تسريب مواضيع امتحان شهادة البكالوريا لسنة 2016، وكذلك منع التشويش على

الحجب المؤقت لمواقع معينة بغرض مواجهة ظرف معين، بحيث يمكن أن يستمر هذا الحجب لساعات أو بضعة أيام، حسب الحالة[1]، وإزالة المحتوى المخالف للنظام العام والمخل به، يعتبر خلاف لسابقه (إجراء الحجب) الذي يسري على منطقة معينة، ويتم إزالة هذا الحجب أحيانا من خلال إستعمال برامج وأساليب مخصصة لهذا الغرض، فحذف أو إزالة هذا المحتوى يؤدي بالضرورة إلى إزالة المادة المخلة بالنظام العام[2].

ثانيا: سلطة الضبط السمعي البصري

نص على تأسيس سلطة الضبط السمعي بصري القانون العضوي رقم 12-05 المتعلق بالاعلام[3]، ونص كذلك هذا القانون على أن مهامها وصلاحياتها وسيرها يحددهم القانون المتعلق بالنشاط السمعي البصري[4]، ونص القانون العضوي السالف الذكر على نشاط الإعلام عبر الانترنت بأنه يتم ممارسته بحرية، وبالمقابل يتم مراقبة صحة المعلومات[5]، حيث صدر المرسوم التنفيذي رقم 20- 332 الذي يحدد كيفيات ممارسة

المترشحين لهذا الامتحان من خلال نشر مواضيع زائفة وإشاعات كاذبة ومغرضة بخصوصها، للتفصيل أكثر أنظر: بلخير محمد آيت عويدة، المرجع نفسه، ص274 – 275.

[1] حايطي فاطيمة، المرجع السابق، ص 43-44.

[2] بلخير محمد آيت عودية، الضبط الإداري للشبكات الإجتماعية الإلكترونية، المرجع نفسه، ص278.

[3] أنظر المادة 64 من القانون العضوي رقم 12- 05 مؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012 المتعلق بالإعلام، ج. ر. ج. ج العدد02، المؤرخة في 21 صفر عام 1433هـ الموافق 25 يناير سنة 2012، ص28 التي تنص: " تؤسس سلطة ضبط السمعي البصري وهي سلطة مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي."

[4] أنظر المادة 65 من القانون العضوي رقم 12- 05 المتعلق بالإعلام، التي تنص على أنه " تحدد مهام مهام وصلاحيات سلطة ضبط السمعي البصري، وكذا تشكيلتها وسيرها بموجب القانون المتعلق بالنشاط السمعي البصري.

[5] أنظر المادة 66 من القانون العضوي رقم 12- 05 المتعلق بالإعلام، التي تنص على أنه " يمارس نشاط الإعلام عبر الانترنت بحرية. ويخضع لإجراءات التسجيل ومراقبة صحة المعلومات، بإيداع تصريح مسبق من طرف المدير المسؤول عن جهاز الإعلام عبر الانترنت. وتحدد كيفيات تطبيق هذه المادة عن طريق التنظيم".

نشاط الإعلام عبر الأنترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني[1]، وهنا يبرز لنا دور التنظيم في تفسير القاعدة القانونية وبيان كيفيات تطبيقها.

وجاء القسم الثاني من المرسوم السالف الذكر تحت عنوان التصريح بصحة المعلومة ومراقبتها والذي تضمن المواد من المادة 22 إلى غاية المادة 31 منه وهذا بغرض مكافحة مختلف أشكال الأخبار المغلوطة والكاذبة وتداول الأخبار الصحيحة فقط في الاعلام الي يكون عبر الانترنت، وألزمت المادة 13 من نفس المرسوم التنفيذي المدير المسؤول عن جهاز الإعلام عبر الانترنت بمكافحة المحتوى غير القانوني من إتخاذه لكافة التدابير والوسائل اللازمة لهذا الغرض وهذا وفقا لما جاء في القانون 12- 05 المتعلق بالإعلام وخاصة المحتوى المتضمن التحريض على الكراهية والعنف أو التمييز على أساس الانتماء الجهوي أو العرقي أو الديني أو الرأي السياسي أو الإيديولوجي أو نوع الجنس، وألزمته بإخطار الجهات المعنية عن أي محتوى مخالف للقانون، حتى تتخذ هذه الجهات الإجراءات المناسبة[2]، ويقوم هذا المدير بدوره بمنع النفاذ لهذا المحتوى غير القانوني أو القيام بسحبه على الفور[3].

وبغرض حماية المعطيات الشخصية للأشخاص من الإعلام عبر الأنترنت فإن المادة 15 من نفس المرسوم التنفيذي السالف الذكر أوجبت على هذا المدير الإلتزام بأحكام القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[4]،

[1] المرسوم التنفيذي رقم 20- 332 المؤرخ في 80 ربيع الثاني عام 1442 الموافق 22 نوفمبر 2020، المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، ج.ر.ج. ج عدد70 الصادرة في 25 نوفمبر 2020.

[2] أنظر المادة 13 من المرسوم التنفيذي رقم 20- 332 المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني.

[3] أنظر المادة 14 من المرسوم التنفيذي رقم 20- 332 المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني.

[4] المادة 15 من المرسوم التنفيذي رقم 20- 332 المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني والتي تنص أنه "يجب على المدير المسؤول عن جهاز الإعلام عبر الانترنت

ويجب على المدير المسؤول عن جهاز الإعلام كذلك الإلتزام بالتوصيات في مجال أمن تكنولوجيا المعلومات[1]، إضافة إلى ذلك فإنه إذا ما وجد محتوى ناجم عن القرصنة أو إختراق للموقع الإلكتروني إثبات هذه المخالفات بأي وسيلة وإبلاغ الجهات المعنية وتوقيف الموقع الإلكتروني مؤقتا إلى غاية تجاوز القرصنة أو الاختراق[2].

ويتجلى الدور الوقائي لهذه السلطة من خلال الصلاحيات الرقابية التي تمارسها بموجب القانون 14- 04 وتحديدًا المادة 55[3]، وذلك من خلال ضمان السهر على إحترام الرقابة على أي برنامج سمعي بصري، أيا كان شكل ووسيلة بثه بغرض مطابقته للقوانين والتنظيمات سارية المفعول[4]، وتمتد صلاحيات هذه الهيئة إلى النشاط السمعي البصري عبر الإنترنت[5]، أي إلى ما يتم بثه وعرضه على القنوات الإلكترونية وعلى مواقع القنوات الإعلامية على مواقع التواصل الاجتماعي "فيسبوك وتويتر وإنستغرام" وعلى "يوتيوب."

حيث لجأ القائمون على الاتصال في المؤسسات الإعلامية التقليدية الراغبين في دخول السباق مع وسائل الإعلام الجديدة إلى تقنيات التدوين المصغر: Twitter وFacebook

---

الإلتزام بالأحكام المنصوص عليها في القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 والمتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي".

[1] أنظر المادة 16 من المرسوم التنفيذي رقم 20- 332 المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني.

[2] أنظر المادة 17 من المرسوم التنفيذي رقم 20- 332 المتضمن تحديد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني.

[3] أنظر المادة 55 من القانون رقم 14- 04 المؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014، المتعلق بالنشاط السمعي البصري، ج.ر.ج. ج عدد 16 الصادرة في 21 جمادى الأولى عام 1435 هـ الموافق 23 مارس سنة 2014.

[4] كهينة سلام، جميلة قادم، الضبط الإعلامي في التشريع الجزائري قراءة في مهام، صلاحيات وخصائص سلطة ضبط السمعي البصري وفق القانون 14-04 المنظم للنشاط السمعي بصري، مجلة الرسالة للدراسات الاعلامية، كلية العلوم الانسانية والاجتماعية، جامعة العربي التبسي، تبسة، الجزائر، المجلد 06، العدد 02، جوان 2022، ص422.

[5] وفقا لنص المادة 56 من القانون 14-04 التي تنص على أنه "تمتد مهام وصلاحيات سلطة الضبط السمعي البصري إلى النشاط السمعي بصري عبر الانترنت عبر الانترنت".

وYouTube، من أجل ضمان أكبر عدد من المتابعين والمتفاعلين وهذا مرده الطبيعة المتغيرة للجمهور[1].

ثالثا: سلطات التصديق الالكتروني

تمثل سلطات التصديق الالكتروني آليات رقابية وقائية، وتتمثل في السلطة الرئيسية وهي السلطة الوطنية للتصديق والتوقيع الالكترونيين، التي تنبثق عنها سلطتين السلطة الإقتصادية للتصديق الإلكتروني والسلطة الحكومية للتصديق الإلكتروني، فالسلطة الوطنية للتصديق الالكتروني هي سلطة إدارية مستقلة، تتمتع بالشخصية المعنوية والإستقلال المالي[2]. والتي تتفرع عنها السلطة الإقتصادية الخاصة بالجانب الاقتصادي[3]، يتم تعيينها من طرف السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية[4] مهمتها الرئيسية متابعة ومراقبة مؤديي خدمات التصديق الالكتروني[5] فهذه الأخيرة تتعامل مع الشركات الخاصة والبنوك والمواطنيين[6]، وكذلك توجد السلطة الحكومية للتصديق الإلكتروني، تتمتع هي الأخرى بالإستقلال المالي والشخصية المعنوية، تنشأ لدى الوزير المكلف بالبريد والتكنولوجيات الإعلام والاتصال، تتمثل مهمتها الرئيسية بمتابعة ومراقبة نشاط التصديق الإلكتروني للأطراف الثالثة الموثوقة وتوفر خدمات التصديق للمتدخلين من الجانب الحكومي[7].

---

[1] بلخير محمد آيت عودية، المرجع السابق، ص207.

[2] أنظر المادة 16 من القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر.ج.ج، العدد 06، الصادرة في 20 ربيع الثاني عام 1436 هـ الموافق 10 فبراير سنة 2015 م.

[3] آمال بوبكر، التصديق الالكتروني في النظام القانوني الجزائري، مجلة المفكر للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، العدد3، سبتمبر 2018، ص215.

[4] أنظر المادة 29 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

[5] أنظر المادة 30 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

[6] آمال بوبكر، المرجع نفسه، ص215.

[7] أنظر المادة 28 من القانون رقم 15-04 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

الفرع الثاني: السلطات الادارية المستقلة للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

هذه السلطات مجالها الوقاية ومكافحة الجرائم المستجدة، والتي تمثل في دراستنا هذه الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث طبيعتها تتمثل في السلطات الإدارية المستقلة، هذا يتجلى من خلال القوانين المنظمة لهذه السلطات والتي تتمثل في دراستنا هذه في: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها (أولا)، والسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي (ثانيا).

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها

ورد الفصل الخامس من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها موسوم ب "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته"، فنصت المادة 13 منه على أنها تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته.

وأنه يتم تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم[1]، لأن هذا القانون لم يفصل فيها وإنما اكتفى فقط بالنص على إنشائها ومهامها، حيث نص في المادة 14 منه على هذه المهام وحدد مهامها على سبيل المثال وهذا ما يستشف من عبارة "**خصوصا**" الواردة في نفس المادة والتي جاءت كما يلي "تتولى الهيئة المذكورة في المادة 13 أعلاه، **خصوصا** المهام الآتية: ..."

[1] أنظر المادة 13 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تم تنظيم تشكيل الهيئة ومهامها بموجب المراسيم التالية على التوالي: المرسوم الرئاسي رقم 15- 261 الصادر في 8 أكتوبر سنة 2015[1]، ثم تم استدراك هذا المرسوم من خلال الجريدة الرسمية العدد37 المؤرخ في 23 رمضان 1438 هـ الموافق 18 يونيو سنة 2017 م[2]، ثم جاء المرسوم الرئاسي رقم 19- 172 مؤرخ في 3 شوال عام 1440 الموافق 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها والذي ألغى جميع الأحكام المخالفة لما ورد فيه، لاسيما أحكام المرسوم الرئاسي الذي سبقه رقم 15- 261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ثم تمت إعادة تنظيمها بموجب المرسوم الرئاسي 20 -183[3]، حيث هذا المرسوم بموجبه تم إلغاء الأحكام المخالفة له التي جاءت في المرسوم الذي سبقه رقم 19- 172، ثم تم إعادة تنظيم هذه الهيئة بموجب المرسوم الرئاسي[4] رقم 21- 439[1] لسنة 2021.

[1] المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج العدد53، المؤرخة في 24 ذو الحجة عام 1436هـ الموافق 8 أكتوبر سنة 2015.

[2] حيث تم استدراك الجريدة الرسمية العدد 53 الصادر في 24 ذي الحجة عام 1436هـ الموافق 8 أكتوبر سنة 2015، الصفحة 19، العمود الأول، المادة 22، الفقرة3، السطر2: - **بدلا من** " ... الرخصة المسلمة من الشرطة القضائية" – **يقرأ** "... الرخصة المسلمة من السلطة القضائية" الباقي دون تغيير

[3] المرسوم الرئاسي رقم 20- 183 مؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ج.ر.ج.ج العدد 40 المؤرخة في 26 ذي القعدة عام 1441 هـ الموافق ل 18 يوليو سنة 2020.

[4] ويجب أن ننوه في هذا الصدد إلى أن صدور مرسوم رئاسي يحدد تشكيلة وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، يعتبر مخالف للمبدأ المكرس في النظام الدستوري والقانوني الجزائري، وذلك لأن الإحالة إلى التنظيم مفادها صدور مرسوم تنفيذي من طرف الوزير الأول، بدلاً من صدور مرسوم رئاسي، وبالتالي في هذه الحالة يعتبر تعديا على إختصاصات الوزير الأول. أنظر خرشي إلهام، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، مخبر

إن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي[2] يتم وضعها لدى رئيس الجمهورية[3]، وما يمكن ملاحظته أن المرسوم الجديد اختلف عن المرسوم الرئاسي السابق رقم 20- 183 في كون السابق نص بأن هذه الهيئة توضع تحت سلطة رئيس الجمهورية[4]. أما مقر الهيئة فإنه يتواجد بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر

دراسات وأبحاث حول المجازر الاستعمارية ومخبر تطبيقات التكنولوجيا الحديثة على القانون، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر، المجلد 04، العدد 01، 2022، ص61.

[1] المرسوم الرئاسي رقم 21- 439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ج.ر.ج.ج العدد 86 المؤرخة في 6 ربيع الثاني عام 1443هـ الموافق ل 11 نوفمبر سنة 2021.

[2] وما يجدر بنا الإشارة إليه في هذا الصدد أن الهيئة في المرسوم الرئاسي رقم 15- 261 المتضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، تم تكيفها فيه على أنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والإستقلال المالي، توضع لدى الوزير المكلف بالعدل، أنظر المادة 2 منه.

ثم في المرسوم الذي ألغاه رقم 19-172، يحدد تشكيلة الهيئة الوطنية للوقاية من تكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها تراجع عن تكييفها بالسلطة الإدارية المستقلة وتم تكيفيها فيه بالمؤسسة العمومية ذات الطابع الإداري تتمتع بالشخصية المعنوية والإستقلال المالي توضع تحت سلطة وزارة الدفاع الوطني. أنظر المادة 2 منه.

ثم في المرسوم الرئاسي الذي أعاد تنظيم الهيئة رقم 20-183 تراجعها عن تكييف بالمؤسسة العمومية ذات الطابع الإداري، وأعاد تكييفها بالسلطة الإدارية المستقلة التي تتمتع بالشخصية المعنوية والإستقلال المالي، ووضعها تحت سلطة رئيس الجمهورية. أنظر المادة 2 منه.

وهو نفسه التكييف الذي إستقر عليه المرسوم الرئاسي رقم 21- 439 لكنه وضعها لدى رئيس الجمهورية. أنظر المادة 2 منه.

[3] أنظر المادة 1 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[4] أنظر المادة 2 من المرسوم الرئاسي رقم 20- 183 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

من التراب الوطني، وذلك بموجب مرسوم رئاسي[1]، وهو نفسه ما جاء في المرسوم الرئاسي المنظم للهيئة السابق.

تتكون الهيئة من مجلس توجيه ومديرية عامة، يوضعان تحت سلطة رئيس الجمهورية[2]، ويقدم مجلس التوجيه والمديرية العامة، لرئيس الجمهورية عرضا عن نشاطاتهما[3]، وهذا يعتبر نوع من الرقابة على نشاط الهيئة وسيرها.

1_ مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها:

تمارس الهيئة المهام المكلفة بها تحت رقابة السلطة القضائية، وذلك طبقا لأحكام قانون الإجراءات الجزائية والقانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[4].

وما يلاحظ أنه في المرسوم الأخير أي المرسوم رقم 21- 439 لسنة 2021 أنه تمت إضافة مصطلح قانون "الإجراءات الجزائية"، حيث جاء فيه أن الرقابة القضائية تكون وفقا لقانون الإجراءات الجزائية وهذا خلاف المرسوم السابق لسنة 2020 الذي لم يحدد القانون وإنما جاء فيه أن الرقابة القضائية تكون طبقا لأحكام التشريع الساري المفعول.

---

[1] أنظر المادة 3 من المرسوم الرئاسي رقم 20- 183، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

أنظر المادة 3 من نفس المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[2] أنظر المادة 5 من المرسوم الرئاسي رقم 21- 439 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 5 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[4] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

من مهام المنوطة بالهيئة والتي تتمثل أهمها في:

أ_ أنها تحدد إستراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ:[1] هذا على خلاف المرسوم السابق الذي كانت فيه الهيئة تقترح فقط عناصر الإستراتيجية الوطنية للوقاية من هذه الجرائم دون تحديدها، وحسنا قعل المشرع بإعادة صياغته لهذه المادة لأنه أوضح نية حقيقية للوقاية من هذه الجرائم ومكافحتها.

ب_ تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:[2] وهي نفس المهمة المكلفة بها في المرسوم السابق.

ج_ تضمن مراقبة الوقائية للاتصالات الإلكترونية، تحت سلطة القاضي المختص، بغرض الكشف عن الجرائم المتصلة بالأعمال الإرهابية أو التخريبية أو التي تمس بأمن الدولة:[3] حيث تمت إضافة في هذا المرسوم أن المراقبة الوقائية للإتصالات الإلكترونية تكون تحت سلطة القاضي المختص وهذا خلافا للمرسوم السابق الصادر في سنة 2020 والذي نص على إعتماد المراقبة الوقائية للكشف عن هذه الجرائم الخطيرة فقط، وحسنا فعل المشرع بجعل المراقبة الوقائية للاتصالات الالكترونية تحت إشراف قضائي، مما يوفر الضمانات القضائية اللازمة.

[1] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[2] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

د_ كما تضمن عمليات المراقبة الالكترونية المتعلقة بأمن الجيش، وتنسق ذلك مع المصالح المختصة لوزارة الدفاع الوطني: وفق نفس الشروط المنصوص عليها في التشريع الجاري العمل به[1]، وما يلاحظ أنه تمت إضافة هذه الفقرة بموجب المرسوم الأخير ولم تكن متواجدة في المرسوم السابق لسنة 2020.

هـ_ تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:[2] ويلاحظ أن هذه الفقرة تختلف عن الفقرة المقابلة لها في المرسوم السابق لسنة 2020، الذي ورد فيه أن تطوير التعاون يكون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال، فالتغيير في هذه الفقرة تمثل في أن التعاون يكون في مجال الوقاية من هذا النوع من الجرائم حيث حددت طبيعة التعاون والذي يكون وقائي.

و_ تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال إختصاصها: وفقا لأحكام المادتين 17 و18 من القانون 09-04، ويلاحظ أن ما تم إضافته في المرسوم الأخير هو أن طلبات المساعدة والتعاون على المستوى الدولي تكون تتوافق مع المادتين 17 و18 من القانون 09- 04.

حيث تكون الإستجابة لطلبات المساعدة القضائية الرامية لتبادل المعلومات أو إتخاذ الإجراءات التحفظية وفقا لما جاءت به الإتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية، ومبدأ المعاملة بالمثل[3]، ويتم رفض تنفيذ هذه الطلبات إذا كانت تمس بالسيادة الوطنية أو النظام العام، وقد يتم تقييد الاستجابة لهذه الطلبات بشروط كشرط وجوب

[1] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[2] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 17 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المحافظة على المعلومات التي تم الإدلاء بها وتبليغه بها، وشرط وجوب استعمالها فقط فيما ورد في الطلب دون الخروج عليه[1].

ز_ تقوم بتجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل إستعمالها في الإجراءات القضائية؛

ح_ المساهمة في تكوين محققين مختصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال؛

ط_ المساهمة في تحيين المعايير القانونية في مجال اختصاصها؛

ي_ مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال: عن طريق جمع المعلومات والتزويد بها وإنجاز الخبرات القضائية[2].

وما يلاحظ أن هذه المهام لم يحدث بشأنها أي تعديل أو تغيير أو إضافة في المرسوم الجديد بل بقيت على حالها كما وردت في المرسوم السابق.

2_ الدور الوقائي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها:

لهذه الهيئة دور وقائي قبل حدوث جريمة من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات فدورها في هذه الحالة سابق لمرحلة وقوع الجريمة، ولها كذلك دور لاحق لمرحلة إرتكاب الجريمة.

أ _ دور توعوي وتحسيسي: يعتبر الجانب التوعوي والتحسيسي من صميم صلاحيات الأجهزة المكلفة بالوقاية، والتي تتمثل في دراستنا في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، فهذه العملية تهدف بشكل أساسي إلى

[1] أنظر المادة 18 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] أنظر المادة 4 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

توعية الناس بخطورة هذا النوع من الجرائم المستحدثة الدرجة الأولى إذكاء وأضرارها على الفرد والمجتمع من جميع النواحي وعلى جميع الأصعدة، وتعليمهم كيفية التعامل مع هذه الجرائم قصد ضمان إشراك جميع شرائح المجتمع في العملية الوقائية[1]، حيث تكفل عملية التوعية مديرية المراقبة الوقائية واليقظة الإلكترونية، فتقوم بتنظيم أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال، وحول المخاطر المتصلة بها[2].

ب_ المراقبة الوقائية للاتصالات الالكترونية:

هذا الإجراء نص عليه القانون القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في الفصل الثاني منه، والذي جاء معنون ب "**مراقبة الإتصالات الإلكترونية**"، وأورد من خلاله المشرع الحالات التي تسمح باللجوء إلى إجراء المراقبة الإلكترونية. وما يلاحظ أن هذا القانون لم يعرف مراقبة الإتصالات الإلكترونية ولا إجراء المراقبة الإلكترونية، وإنما اكتفى فقط بتعريف الإتصالات الإلكترونية في المادة الثانية منه على أنه "أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[3]، أما المادة الثانية من قانون حماية الأشخاص الطبيعيين في مجال حماية المعطيات ذات الطابع الشخصي رقم 18-07 فإنها عرفتها "كل إرسال أو تراسل أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات، مهما كانت طبيعتها، عبر

[1] سوماتي شريفة، السياسة الجنائية للمشرع الجزائري في مواجهة الجريمة المستحدثة، رسالة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 1، الجزائر، 2017- 2018، ص130.

[2] أنظر المادة 14 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 02 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية"[1] وهو نفس التعريف الذي ورد في المادة 10 من قانون البريد والإتصالات الإلكتروني 18-04[2].

وما يجدر بنا الإشارة إليه أن القانون 09-04 أدرج إجراء المراقبة الإلكترونية ضمن التدابير الوقائية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، إضافة إلى اعتبارها إجراء من إجراءات الحصول على الأدلة الرقمية[3].

_ حالات مراقبة الاتصالات الالكترونية الوقائية:

للمراقبة حالتين: الحالة الاولى تتم من خلال منح الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته إختصاص الحصري لمراقبة الإتصالات الالكترونية:

حيث يؤول للهيئة الإختصاص الحصري بقصد الوقاية من الأفعال الموصوفة بجرائم الإرهاب والتخريب أو التي تمس بأمن الدولة ومكافحتها، حيث تقوم بمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها أي تكون المراقبة على المعطيات المتحركة المتواجدة داخل منظومة معلوماتية تحت سلطة قاض لدى الهيئة، وذلك وفقا لأحكام المادة 04 من القانون 09-04، وتخضع إجراءات التفتيش والحجز لأحكام قانون الإجراءات الجزائية[4] أي وفقا للقواعد العامة، وبالتالي فهذه المراقبة تكون وقائية أي قبل حدوث الجريمة.

---

[1] أنظر المادة 02 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعين في مجال حماية المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 10 من القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018، يحدد القواعد المتعلقة بالبريد والإتصالات الإلكترونية، ج. ر.ج.ج، العدد 27، المؤرخة في 27 شعبان عام 1439 الموافق ل 13 مايو سنة 2018.

[3] الطيب بلواضح، المرجع السابق، ص187.

[4] أنظر المادة 25 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

وعليه فهذه المراقبة تتميز بالطابع الوقائي حيث يتم إعتمادها قبل حدوث أي جريمة وذلك بغرض تفادي وقوعها، ونظرا لخطورة هذا الإجراء الوقائي كونه يمس بحرمة وسرية المراسلات والاتصالات تم حصر إستخدامه من طرف المشرع في حالة الوقاية من الجرائم الارهابية والتخريبية والماسة بأمن الدولة كما إشترط لاستعمالها صدور إذن من النائب العام لمجلس قضاء الجزائر[1]. فتقوم الهيئة بهذا النوع من المراقبة الوقائية أو الاستباقية، حيث تنفذ هذه المهمة مديرية المراقبة الوقائية واليقضة الإلكترونية، فتقوم بعمليات المراقبة الوقائية للإتصالات الإلكترونية، بغرض الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وذلك بناء على إذن مكتوب من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول[2]. لأنه بعد وقوع الجريمة ينعقد الاختصاص للسلطة القضائية المختصة[3].

أما الحالة الثانية: حالة توفر معلومات عن اعتداء محتمل على المنظومة معلوماتية بشكل يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[4].

[1] حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، مخبر السياسات العامة وتحسين الخدمة العمومية بالجزائر، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 05، العدد 03، ديسمبر 2021، ص468.

[2] أنظر المادة 14 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] خرشي إلهام، المرجع السابق، ص69.

[4] أنظر المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

_ شروط المراقبة الوقائية للإتصالات الالكترونية:

_ عدم وجود جريمة مرتكبة فعلاً وإنما مجرد إحتمال الاعتداء عن نظام معلوماتي بشكل يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني: حيث تكون المراقبة الوقائية للإتصالات الإلكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ؛

_ مراقبة الإتصالات الالكترونية وتجميع وتسجيل محتواها في حينها داخل منظومة معلوماتية[1]: أي تكون في زمن البث المباشر[2]، على المعطيات المتحركة وليست على البيانات الثابتة؛

_ ضرورة الحصول على إذن مكتوب من السلطة القضائية المختصة[3]، للقيام بإجراء المراقبة في جميع الحالات الواردة في المادة 04 من القانون 09- 04؛

_ شرط توفر إذن مكتوب من السلطة القضائية المختصة، بخصوص الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة السلطة القضائية المختصة بمنح الإذن تتمثل في النائب العام لدى مجلس قضاء الجزائر، الذي يمنح ضباط الشرطة القضائية الذين ينتمون للهيئة إذنا لمدة (06) أشهر قابلة للتجديد، وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها، وتكون هذه الترتيبات التقنية الموضوعة لغرض الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة موجهة **حصريا** لتجميع وتسجيل معطيات ذات الصلة ذات الصلة

[1] أنظر المادة 25 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[2] حابت أمال، المرجع السابق، ص 469.

[3] أنظر المادة 4 من القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

بالوقاية من الأفعال الإرهابية والاعتداءات على وأمن الدولة ومكافحتهما، وذلك تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير[1].

_الأحكام الإجرائية للمراقبة الوقائية للإتصالات الالكترونية : للهيئة لأجل القيام بعملية مراقبة الاتصالات الإلكترونية، وضع وحدة أو أكثر، مزودة بالوسائل والمعدات الفنية والتقنية اللازمة، حيث بعد الحصول على ترخيص من السلطة القضائية لصالح ضباط الشرطة القضائية، يتولى أعوان الهيئة ووحدتها المكلفة بالمراقبة، الجوانب التقنية، وذلك بتوجيه وإشراف أحد قضاة الهيئة، وبالاستعانة بالضابط من الشرطة القضائية التابع للهيئة، وتسجل الوحدة أعمالها في محاضر محررة وفقاً لأحكام قانون الإجراءات الجزائية[2]. ثم تحفظ الهيئة المعلومات المتحصل عليها أثناء عمليات المراقبة[3]، ثم يتم تسجيل الاتصالات الإلكترونية الخاضعة للمراقبة، وتحرر وفقا لما هو منصوص عليه في قانون الإجراءات الجزائية، ثم تُسلم هذه التسجيلات والمحررات إلى الشرطة القضائية المختصة، التي تحتفظ دون غيرها بهذه المعطيات طِوال المدة القانونية المنصوص عليها قانونا[4]. ويتم استخدام الإتصالات الالكترونية والمعلومات والمعطيات التي تستلمها أو تجمعها الهيئة، حصرًا إلا لغرض الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وفقا لما نص عليه القانون رقم 09-04، دون سواه، تحت طائلة العقوبات الجزائية[5]. وما يجدر بنا الإشارة إليه أنه

[1] أنظر المادة 4 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] أنظر المادة 26 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 27 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[4] أنظر المادة 28 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[5] أنظر المادة 29 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

يجوز للهيئة الاستعانة بموظفين مختصين من الوزارات المختصة في مجال تكنولوجيات الإعلام والاتصال، وبخبراء أو أشخاص لمساعدتها في عملها[1].

الوسائل والتجهيزات التقنية التي تُستخدم لمراقبة الاتصالات الإلكترونية تستعملها وتحوزها وتقتنيها وتستوردها إلا الهيئة في إطار إختصاصها[2]، ويجوز للقضاة وضباط الشرطة القضائية التابعين لها، عند أو في معرض ممارستهم لمهامهم تفتيش أي مكان جهاز، يكونون على علم بأنه يحوز و/أو يستخدم وسائل وتجهيزات تُستخدم لمراقبة الاتصالات الإلكترونية، وذلك حسب ما هو مقرر في قانون الإجراءات الجزائية. ويستثنى من ذلك المنشآت التابعة لوزارة الدفاع الوطني، وإذا كانت هذه الأفعال تشكل وصفها جزائيا، يتم إخطار وكيل الجمهورية المختص للقيام بإجراءات المتابعة[3].

ونظرا لخطورة هذا الإجراء ومساسه بالحقوق الأساسية المكفولة بموجب الصكوك الدولية والدساتير الوطنية وأهمها الحق في الحياة الخاصة فإن المراقبة الوقائية للاتصالات الالكترونية تجد مبررها في كونها محصورة في نطاق نوع خاص من الجرائم التي تتميز بخطورتها على الجماعة وهي الجرائم الارهابية والتخريبية أو الجرائم الماسة بأمن الدولة[4].

وما يجدر ذكره أن المراقبة الإلكترونية إضافة إلى أنها إجراء وقائي تعتبر إجراء مستحدث في التحري والتحقيق.

---

[1] أنظر المادة 32 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[2] أنظر المادة 33 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[3] أنظر المادة 30 من المرسوم الرئاسي رقم 21- 439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

[4] عائشة عبد الحميد، الإطار القانوني للترصد الإلكتروني الوقائي كإطار للإصلاح القضائي في الجزائر، مجلة التراث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 11، العدد 05، ديسمبر 2021، ص34.

_ آليات مراقبة الإتصالات الإلكترونية التقنية والفنية:

_ التسرب الإلكتروني: سنتطرق إليه لاحقا بالتفصيل

_ حفظ المعطيات المتعلقة بحركة السير: وهذه المعطيات عرفتها المادة 2 من القانون 09-04، فهي تتمثل في أي معطيات متعلقة بالاتصالات عن طريق منظومة معلوماتية تنتهجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الإتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة[1]، والإلتزام بحفظ هذه المعطيات نصت عليه المادة 11 من نفس القانون.

وهناك آليتين نص عليهما المشرع الفرنسي ولم ينص عليهما المشرع الجزائري يتمثلان في إلتقاط المعطيات وفتح المعطيات المشفرة.

ج_ تفتيش النظم المعلوماتية الوقائي والحجز الوقائي:

من إختصاص الهيئة الوقائي كذلك تفتيش المنظومة المعلوماتية[2]، والمادة 4 التي أحالتنا إليها المادة 5 من القانون 09-04 نصت على حالات إمكانية القيام بعمليات المراقبة الالكترونية، وبالتالي يمكن القيام بالتفتيش كذلك بغرض الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذلك في حال توفر معلومات عن احتمال اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو

[1] أنظر المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] المادة 5 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش، ولو عن بعد إلى:

أ_ منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها

ب_ منظومة تخزين معلوماتية..."

الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[1]، فما يلاحظ أن المشرع سمح بالتفتيش الوقائي في هذين الحالتين، وكذلك في هاتين الحالتين يمكن القيام بإجراء الحجز الوقائي داخل المنظومة المعلوماتية[2]. وما يلاحظ أن المشرع الجزائري خرج على ما هو متعارف عليه، عندما نص على إمكانية القيام بإجراء المراقبة الالكترونية والتفتيش الالكتروني والحجز الالكتروني كإجراءات وقائية بهدف منع وقوع الجريمة، على خلاف ما هو متعارف عليه في القواعد العامة التي تشترط لتطبيق هذه الإجراءات الماسة بالحياة الخاصة وقوع الجريمة[3]، لكن ما يجدر بنا الإشارة إليه هو أن المشرع لم ينص على قواعد خاصة لتطبيق هذه الإجراءات الوقائية، وإنما نص على القواعد المنظمة لها إذا تم تطبيقها في مرحلتي البحث والتحري والتحقيق تكون وفقا لقانون الإجراءات الجزائية، كان من المستحسن لو خصها بقواعد خاصة إذا تم إتخاذها كإجراءات وقائية كونها ماسة بالحياة الخاصة، ومن المستحسن لو خص بها هيئة قضائية لتنفيذها.

وما يجدر بنا الإشارة إليه بخصوص الوقاية من الجرائم المعلوماتية فإنه أصبحت تستخدم البيانات الضخمة والذكاء الإصطناعي في التنبؤء بالجرائم المعلوماتية قبل إرتكابها.

[1] أنظر المادة 4 الفقرتين أ وب من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] أنظر المادة 3 والمادة 4 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] سوماتي شريفة، السياسة الجنائية للمشرع الجزائري في مواجهة الجريمة المستحدثة، المرجع السابق، ص 103.

ثانيا: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

1_ مفهوم السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

إن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي[1] تعتبر الهيئة الرسمية المناط لها حماية المعطيات الشخصية في الجزائر، هذا ما يضفي الشفافية في مجال إستعمال المعطيات سواء في المؤسسات العامة أو الخاصة، حيث يضمن التوازن بين حماية هذه المعطيات وإستعمال المؤسسات لها في أنشطتها[2]، وأكدت المادة 22 من القانون 18-07 على إستقلالية هذه السلطة الإدارية، فهي تتمتع بالشخصية المعنوية، تضع هذه السلطة نظامها الداخلي والذي تحدد من خلاله كيفيات تنظيمها وسيرها، يقع مقرها في الجزائر العاصمة[3]، وعليه فالمشرع الجزائري امتاز بالوضوح في تحديد التكييف القانوني لهذه السلطة الوطنية، وهذا بغرض تفادي الغموض حول طابعها الإداري ودورها كهيئة ضبط في مجال المعطيات الشخصية[4]، تشكيلتها متنوعة[1]، ويتم تعيين كل من رئيسها وأعضائها بموجب مرسوم رئاسي لمدة 5 سنوات قابلة للتجديد[2].

---

[1] المشرع الجزائري حذا حذو الاتجاه الذي سايره المشرع الفرنسي من خلال إنشاء هذا الأخير لهيئة إدارية مستقلة لا تخضع لأي سلطة رئاسية سميت ب:« La **Commission nationale de l'informatique et des libertés (CNIL)** » "اللجنة القومية للمعلوماتية والحريات"

Article 11 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Modifié par Loi n°2004-801 du 6 août 2004 - art. 3 JORF 7 août 2004 « La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante. Elle exerce les missions suivantes… »

[2] كهينة قونان، نوارة حمليل، السلطة الوطنية كهيئة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 18-07، مجلة الدراسات القانونية، مخبر السيادة والعولمة، كلية الحقوق والعلوم السياسية، جامعة يحى فارس، المدية، الجزائر، المجلد 07، العدد02، جوان 2021، ص 565- 566.

[3] أنظر المادة 22 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] تبينة حكيم، آليات الضبط الإداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة، الجزائر، المجلد 58، العدد 01، 2021، ص 226.

وتضطلع السلطة الوطنية حسب ما حددته المادة 25 من القانون نفسه بجملة من المهام من بينها: المراقبة القانونية من خلال السهر على مطابقة ومعالجة المعطيات ذات الطابع الشخصي لأحكام القانون وضمان عدم انطواء تكنولوجيا الإعلام و الاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والخاصة[3]، وكذلك لها مهمة الإعلام والحماية عن طريق تعزيز استخدام التقنيات بطريقة تحمي الخصوصية، عبر تشجيع تقنيات التشفير، والمواكبة وتقديم المشورة من خلال مساعدة وإلزام المهنيين بالتقيد بأحكام قانون حماية المعطيات الشخصية[4]، وذلك بتقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة[5]، ولها مهام تلقى الشكاوى، ولها سلطة التأديب حيث تكلف أعضائها لتحقق من مدى التزام المؤسسات والشركات المعنية بمعالجة البيانات الشخصية وفقا للقانون، وباحترام حقوق الأفراد وحرياتهم[6]، وتوقيع العقاب وقمع المخالفات حيث تصدر عقوبات إدارية وفقا لأحكام المادة 46 من هذا القانون، كذلك تمنح الترخيصات وتتلقى

---

[1] وفقا للمادة 23 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي تتشكل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي ثلاث أشخاص مختصين في مجال عمل السلطة من بينهم رئيسها يختارهم رئيس الجمهورية، و ثلاثة قضاة باقتراح من المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من البرلمان يتم اختيارهم من قبل رئيس كل غرفة، إضافة إلى ممثل واحد عن كل من المجلس الوطني لحقوق الإنسان، وعن وزير الدفاع الوطني، وعن الوزير المكلف بالداخلية، وعن وزير العدل حافظ الأختام، وعن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيا الرقمية، وعن وزير الصحة، وعن وزير العمل والتشغيل والضمان. ويتم اختيار أعضائها حسب اختصاصهم القانوني و/أو التقني المعطيات ذات الطابع الشخصي. ويمكن لهذه السلطة الاستعانة بأي شخص مؤهل يمكنه مساعدتها.

[2] أنظر المادة رقم 23 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] العيداني محمد يوسف، المرجع سابق، ص 123.

[4] منى الأشقر جبور، محمود جبور، المرجع السابق، ص158.

[5] المادة 25 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[6] منى الأشقر جبور، محمود جبور، المرجع نفسه، 159.

التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، كالترخيص بنقل المعطيات نحو الخارج وفقا للشروط المنصوص عليها في القانون 18-07، وتقوم كذلك بنشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من القانون 18-07[1]، وتقدم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات، وتطوير علاقة التعاون مع السلطات الأجنبية المماثلة، كما تعد السلطة تقريرا سنويا مفصلا إلى رئيس الجمهورية حول جميع نشاطاتها. ويلتزم رئيس السلطة وأعضائها بالمحافظة على الطابع السري للمعطيات أثناء تأدية مهامهم وبعد الانتهاء منها[2].

وما يجدر بنا الإشارة إليه في هذا الصدد أنه تم تنصيب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي يوم الخميس 11 أوت 2022[3]. وسيتم التطبيق الفعلي للقانون 18-07 قبل نهاية أوت 2023 وفقا لما نصت عليه المادة 75 من القانون السالف الذكر[4].

---

[1] المادة 25 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] العيداني محمد، يوسف زروق، المرجع سابق ، ص 123.

[3] كما تتدرج عملية التنصيب في إطار انخراط دولة الجزائر في جميع المواثيق والعهود والاتفاقيات الدولية التي تتعلق بحماية حقوق الإنسان وذلك بهدف إنشاء مؤسسات تلبي المعايير الدولية

وللإشارة، فقد تم تعيين أعضائها لعهدة مدتها خمس سنوات بموجب _المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، ج.ر.ج.ج العدد 35، المؤرخة في 23 شوال 1443 الموافق 18 ماي.

وقد جرت مراسم التنصيب برئاسة الرئيس الأول للمحكمة العليا، السيد الطاهر ماموني، وبحضور رئيس المحكمة الدستورية، السيد عمر بلحاج، ومستشار رئيس الجمهورية المكلف بالشؤون القانونية والقضائية، السيد بوعلام بوعلام، ووزير العدل حافظ الأختام، السيد عبد الرشيد طبي، ورئيسة مجلس الدولة، السيدة فريدة بن يحيى، ورئيس المجلس الوطني لحقوق الإنسان، السيد عبد المجيد زعلاني.

متوفر على الرابط التالي: https://www.aps.dz/ar/algerie/130309-2022-08-11-16-30-37 تم الإطلاع عليه بتاريخ 08/14/ 2022 على الساعة 21:59.

[4] الموقع الرسمي للسلطة الوطنية لحماية المعطيات الشخصية، متوفر على الرابط التالي:

2_ الإجراءات المسبقة عن المعالجة كآلية وقائية لحماية المعطيات ذات الطابع الشخصي.

للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي دور مهم في الوقاية من المساس بالمعطيات الشخصية من خلال، ويتجلى ذلك من خلال الرقابة القبلية والبعدية لعمليات المعالجة من خلال طلب التصريح المقدم لها، والتراخيص التي تقدمها. ويعتبر كل من إجراء التصريح والترخيص بمثابة شرطين أساسيين إلزاميين للمعالجة[1] إضافة إلى شرط الموافقة المسبقة للمعني.

أ_ التصريح:

ويكون التصريح المسبق بمعالجة المعطيات ذات الطابع الشخصي لدى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث يتضمن هذا التصريح الإلتزام بإجراء المعالجة وفقا للقانون 18-07، ويمكن أن يقدم هذا التصريح إلكترونيا أو ورقيا، وكذلك الأمر بالنسبة لوصل الإيداع فإنه يُسلم للمسؤول عن المعالجة، أو يُرسل إليه بالطريق الإلكتروني فورا في أجل أقصاه 48 ساعة[2]. ومع التحول إلى الادارة الالكترونية فإنه يمكن تخفيف العبء على المسؤول عن المعالجة، وإرساله للتصريح أو استلامه لوصل التصريح إلكترونيا.

---

https://anpdp.dz/%d9%85%d8%aa%d9%89-%d9%88-%d8%b9%d9%84%d9%89-%d9%85%d9%86-%d9%8a%d8%b7%d8%a8%d9%82-%d8%a7%d9%84%d9%82%d8%a7%d9%86%d9%88%d9%86-%d8%b1%d9%82%d9%85-18-07-%d8%9f/

تم الإطلاع عليه بتاريخ 15/08/ 2022 على الساعة 07:45.

[1] أنظر المادة 12 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر الفقرة 1 و 2 من المادة 14 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

ووفقا لما نصت عليه المادة 13 من القانون18-07 في الفقرة 3 و4 فإنه في حالة ما إذا كانت المعالجة تابعة لنفس المسؤول عن المعالجة ولها نفس الأغراض أو أغراضها مرتبطة، فيمكن تقديم سوى إعلان واحد إلى السلطة الوطنية ويباشر المسؤول عن المعالجة تحت مسؤوليته عملية المعالجة فور استلامه الوصل الذي نصت عليه نفس المادة[1] ويتضمن التصريح مجموعة من البيانات الإلزامية التي تنصت عليها المادة 14 من القانون 18-07[2]، وما يجب الإشارة إليه أنه يعفى من التصريح المعالجات التي تهدف إلى مسك سجل مفتوح للاطلاع من قِبل الجمهور، أو كل شخص يقوم بإثبات أن له مصلحة مشروعة في ذلك[3].

ب_ الترخيص:

عند تقديم التصريح للسلطة الوطنية من طرف المسؤول عن المعالجة، وعند دراسته يتضح لها، أن هذه المعالجة موضوع التصريح المعتزم القيام بها تنطوي على أخطار ظاهرة، فيما يتعلق باحترام وحماية الحياة الخاصة، والحقوق والحريات والحقوق الاساسية للأشخاص، في هذه الحالة تخضع السلطة الوطنية المعالجة لنظام الترخيص.

يجب تسبيب قرار السلطة الوطنية بالترخيص، وتبليغه للمسؤول عن المعالجة في غضون العشرة (10) أيام من تاريخ إيداع هذا التصريح[4]، الأصل أنه يمنع معالجة المعطيات الحساسة وفقا للقانون 18-07 إلا أنه وإستثناءا يمكن منح الترخيص لغرض

[1] أنظر المادة 13 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] المادة 14 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 16 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] أنظر المادة 17 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

معالجة هذا النوع من المعطيات في حالة ما إذا كانت معالجتها لأسباب متعلقة بالمصلحة العامة، وإذا كانت بناءا على الموافقة الصريحة لصاحبها، وإذا وجد نص قانوني ينص على ذلك، أو الحصول على ترخيص من السلطة الوطنية. ويمكن أن يتم منحه في حالات أخرى ينص عليها القانون حصرا[1].

وطلب الترخيص مثله مثل التصريح يتضمن نفس المعلومات التي أوردتها المادة 14 من القانون 18-07 التي سبق ذكرها، تتخذ السلطة الوطنية قرارها في أجل شهرين من تاريخ إخطارها، ويمكن تمديد هذا الأجل لنفس المدة بقرار مسبب لرئيسها، ويعتبر عدم رد السلطة الوطنية في الأجل المذكور في هذه المادة رفضا للطلب[2]، ويمكن للسلطة إذا كانت المعالجة لها نفس الأغراض وتتعلق بمعطيات مماثلة وبنفس فئات المرسل إليهم، تسلم ترخيص واحد لنفس الطالب[3].

[1] أنظر المادة 18 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[2] أنظر المادة 20 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[3] أنظر المادة 21 من القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

المبحث الثاني: القواعد الجزائية الإجرائية المستحدثة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن الخصوصية التي تتميز بها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، جعلت الإجراءات التقليدية الواردة في قانون الإجراءات الجزائية عاجزت على مكافحة هذه الجرائم، لأن من أبرز المشكلات التي أفرزتها هذه الجرائم هي التحديات الإجرائية من حيث البحث والتحري والتحقيق والمحاكمة خاصة وأن هذه الجرائم لا تعترف بالحدود، مما جعل المشرع الجزائري يستحدث قواعد جزائية إجرائية تتناسب مع البيئة الرقمية التي تُرتكب فيها هذه الجرائم وخصوصيتها العابرة للحدود الوطنية، وفقا لمتطلبات السياسة الجنائية المعاصرة.

وتتمثل في القواعد الجزائية الإجرائية المستحدثة للبحث والتحري والتحقيق عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (المطلب الأول)، استحداث جهات قضائية ذات إختصاص موسع للمتابعة والتحقيق والمحاكمة في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تعديلها (المطلب الثاني).

المطلب الأول: القواعد الجزائية الإجرائية المستحدثة للبحث والتحري والتحقيق عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تم إستحداث نصوص قانونية إجرائية للبحث والتحري والتحقيق عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، نص قانون الإجراءات الجزائية على جملة من القواعد الإجرائية لمكافحة الجرائم بصفة عامة، لكنها لم تكن كافية، فتم استحداث قواعد جديدة تتمشى وطبيعة هذه الجرائم، وتم استحداث أخرى في القانون 09-04.

فمن خلال هذا المطلب سنتعرض إلى القواعد الإجرائية المستحدثة في قانون الإجراءات الجزائية (الفرع الأول)، وإلى القواعد الإجرائية المستحدثة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في القانون رقم 09- 04 (الفرع الثاني).

الفرع الأول: القواعد الإجرائية المستحدثة في قانون الإجراءات الجزائية

في مرحلة البحث والتحري عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أورد قانون الإجراءات الجزائية قواعد قانونية جديدة تتماشى مع طبيعة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، فاستحدث إختصاصات إستثنائية مخولة للشرطة القضائية في مرحلة البحث والتحري عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات (أولا)، ونص على أساليب التحري الخاصة (ثانيا).

أولا: الإختصاصات الإستثنائية المخولة للشرطة القضائية في مرحلة البحث والتحري عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

تم توسع اختصاصات ضباط الشرطة القضائية، إذا ما تعلقت التحريات الأولية أو البحث التمهيدي الذي يقومون بإجرائه بإحدى الجرائم الخطيرة المحددة على سبيل الحصر في قانون الإجراءات الجزائية، والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فبموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، وهذا بغرض تسهيل إجراءات البحث والتحري عن هذا النوع من الإجرام المستحدث وكشف مرتكبيه الذين يتميزون بالذكاء مقارنة مع مجرمي الإجرام التقليدي، وكذلك لأجل جمع الإستدلالات عنه، حتى يتمكن من مواجهة الصعوبات والتحديات التي تعترضه، وذلك نظرًا لخطورة هذه الجريمة، وطبيعتها الخاصة ويستخدم مرتكبيها للأنترنت ووسائل الاتصال الحديثة للتواصل مع بعضهم البعض[1].

[1] محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2018، ص 204- 205.

1_تمديد الإختصاص المكاني للشرطة القضائية إلى كامل الإقليم الوطني في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

حسب القاعدة العامة فالإختصاص المكاني للشرطة القضائية يتحدد في الحدود التي يباشرون فيها وظائفهم المعتادة[1]، وذلك وفقا للمعايير والضوابط الأساسية، وبالتالي فكل إجراء يتم خارج الإختصاص يعتبر باطلا ولا يعتد به قانونا[2]، إلا أن قانون الإجراءات الجزائية خرج عن هذه القاعدة العامة فقرر لضباط الشرطة القضائية مهما كانت جهة انتمائهم الأصلية إختصاصا مكانيا وطنيا في البحث والتحري ومعاينة بعض الجرائم المحددة على سبيل الحصر بموجب نفس المادة السابقة الذكر في فقرتها السابعة[3]، حيث نصت على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من بين هذه الجرائم التي حددتها على سبيل الحصر[4]، ويعمل ضباط الشرطة القضائية في هذه الحالة تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات[5].

[1] أنظر المادة 16 من القانون رقم 06- 22 المؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر سنة 2006، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، ج.ر.ج.ج، العدد84، المؤرخة في 4 ذو الحجة عام 1427 الموافق 4 ديسمبر 2006.

[2] بن سليمان محمد الأمين، خلفي عبد الرحمان، الإجراءات الإستثنائية في جرائم الفساد على ضوء القانون الإجرائي الجزائي الجزائري، مجلة الدراسات حول فعلية القاعدة القانونية، مخبر البحث حول فعلية القاعدة القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، المجلد 04، العدد01،2020، ص143.

[3] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2017/ 2018، ص 285.

[4] أنظر الفقرة 7 من المادة 16 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[5] أنظر الفقرة 8 من المادة 16 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

2_ تمديد التوقيف للنظر في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

كضمانة لعدم التعسف في اتخاذ إجراء التوقيف للنظر نص الدستور الجزائري في المادة[1] 45 من دستور سنة 2020 على أنه "يخضع التوقيف للنظر في مجال التحريات الجزائية للرقابة القضائية، ولا يمكن أن يتجاوز مدة ثمان وأربعين (48) ساعة...

لا يمكن تمديد التوقيف للنظر، إلا استثناء، ووفقا للشروط المحددة بالقانون..."[2]

والمادة 51 من الأمر 15-02 المعدل والمتمم لقانون الإجراءات الجزائية المؤرخ في 23 يوليو 2015 أكدت على عدم جواز تجاوز مدة التوقيف للنظر ثمان وأربعين(48) ساعة كأصل عام، إلا أنه واستثناءا نصت على أنه يمكن تمديد آجال التوقيف للنظر بإذن مكتوب من طرف وكيل الجمهورية المختص مرة واحدة عندما يتعلق الأمر بجرائم الإعتداء على أنظمة المعالجة الآلية للمعطيات، ويجوز بصفة استثنائية منح ذلك الإذن بقرار مسبب دون أن يتم تقديم الشخص إلى النيابة العامة[3]، وما يجدر بنا الإشارة إليه هو في حالة ما إذا كان الموقوف للنظر طفل فإن هذا الإجراء يطبق فقط على الطفل البالغ من العمر 13 سنة ويكون إلا في الجنح التي يكون الحد الأقصى للجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات فيها للعقوبة يزيد عن 5 سنوات حبسا، ولا يمكن أن تتجاوز مدة التوقيف للنظر

[1] علي شملال، المستحدث في شرح قانون الإجراءات الجزائية، الكتاب الأول الاستدلال والاتهام، ط 4، دار هومه، 2019-2020، الجزائر، ص46.

[2] أنظر المادة 45 من التعديل الدستوري لسنة 2020. وفي المادة 60 من التعديل الدستوري لسنة 2016.

[3] أنظر المادة 51 من الأمر 15-02 المؤرخ في 07 شوال عام 1436 الموافق 23 يوليو سنة 2015، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 40، االمؤرخة في 7 شوال عام 1436 الموافق 23 يوليو سنة 2015.

24 ساعة أي نصف المدة المقررة للشخص البالغ، ويمدد بالنسبة له التوقيف للنظر وفقا لما سبق ذكره في هذه الجريمة، وكل تمديد كذلك لا يتجاوز 24 ساعة[1].

3_ الخروج عن الميقات القانوني للتفتيش ولدخول المساكن لوضع الترتيبات التقنية في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

يمكن لضابط الشرطة القضائية بخصوص هذا النوع من الإجرام أي الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أن يجري عملية التفتيش في أي وقت ليلا أو نهارا وهذا ما نصت عليه الفقرة 3 من المادة 47 من ق.إ.ج.ج[2]. ويجوز كذلك الخروج عن الميقات القانوني لدخول المساكن لوضع الترتيبات التقنية بخصوص الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أن المادة 65 مكرر 5 ورد فيها أنه اذا تعلق الأمر بهذا النوع من الجرائم فإن الإذن الممنوح بغرض وضع الترتيبات التقنية يسمح بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 ق.إ.ج.ج ، ويكون ذلك بغير رضا أو علم الأشخاص الذين لهم الحق على تلك الأماكن، وما يجدر بنا الإشارة إليه أن وكيل الجمهورية يراقب مباشرة جميع العمليات التي منح فيها الإذن على هذا

[1] تنص المادة 48 من القانون رقم 15-12 المتعلق بحماية الطفل على أنه: "لا يمكن أن يكون محل توقيف للنظر، الطفل الذي يقل سنه عن ثلاث عشر (13) سنة المشتبه في ارتكابه أو محاولة ارتكابه جريمة."

وتنص المادة 49 من القانون رقم 15-12 المتعلق بحماية الطفل على أنه: " إذا دعت مقتضيات التحري الأولي ضابط الشرطة القضائية أن يوقف للنّظرِ الطفل الذي يبلغ سنه ثلاث عشرةَ (13) سنةً ويشتبه أنه ارتكب أو حاول ارتكاب جريمة، عليه أن يُطلع فورًا وكيل الجمهورية ويُقدم له تقريرًا عن دواعي التوقيف للنظر.

لا يمكن أن تتجاوز مدة التوقيف للنظر أربعًا وعشرين (24)، ولا يتم إلا في الجنح التي تشكل إخلالاً ظاهرًا بالنظام العام، وتلك التي يكون الحد الأقصى للعقوبة المقررة فيها يفوق خمس (5) سنوات حبسا، وفي الجنايات يتم تمديد التوقيف للنظر وفقًا للشروط والكيفيات المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون كل تمديد للتوقيف للنظر لا يمكن أن يتجاوز أربعًا وعشرين (24) ساعة في كل مرة.

إن انتهاك الأحكام المتعلقة بآجال التوقيف للنظر، كما هو مبين في الفقرات السابقة، يُعرض ضابط الشرطة القضائية للعقوبات المقررة للحبس التعسفي".

[2] محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، المرجع السابق، ص 207- 208.

الأساس، وتتم من خلال الحصول على إذن من قاضي التحقيق وتكون تحت رقابته المباشرة في حالة ما إذا أما إذا كان قد تم فتح تحقيق قضائي[1].

ثانيا: أساليب التحري الخاصة المنصوص عليها في قانون الإجراءات الجزائية

تتمثل أساليب التحري الخاصة فيما يلي:

1 _ اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

ويكون ذلك من خلال استخدام كاميرات خفية أو أجهزة تصنت، لكن يجب أن يتم ذلك في إطار إحترام الشرعية الإجرائية، احتراما للحياة الخاصة للإنسان[2]، حيث نصت المادة 47 من التعديل الدستوري لسنة 2020 على أنه "لكل شخص الحق في حماية حياته الخاصة وشرفه[3]. لكل شخص الحق في سرية اتصالاته الخاصة في أي شكل كانت[4].

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية[5]..."[6]، فنظرا لخطورة هذه الإجراءات ومساسها بالحياة الخاصة التي تعتبر محمية دستوريا، فإن المشرع الجزائري حصر مجال تطبيق هذه الإجراءات على فئات جرائم محددة على سبيل الحصر والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[1] أنظر المادة 65 مكرر 5 من ق. إ.ج.ج.

[2] ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، 2018، ص 70.

[3] قبل تعديل هذه الفقرة كانت في دستور 2016 نصت عليها المادة 46 في فقرتها الأولى كالتالي: "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميها القانون".

[4] قبل تعديل هذه الفقرة كانت في دستور 2016 نصت عليها المادة 46 في فقرتها الثانية كالتالي: " سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

[5] قبل تعديل هذه الفقرة كانت في دستور 2016 نصت عليها المادة 46 في فقرتها الثالثة كالتالي: " لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم".

[6] أنظر المادة 47 من التعديل الدستوري لسنة 2020.

والمشرع لم يعرف هذه الإجراءات في قانون الإجراءات الجزائية الجزائري، بل اكتفى بالنص على أحكامها ضمن الفصل الرابع المعنون ب : "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، والمقصود باعتراض المراسلات هي "عملية مراقبة سرية المراسلات السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة"[1]، أما تسجيل الأصوات والتقاط الصور فهي تسجيل المحادثات الشفهية التي يجريها الأشخاص ولا سيما بصفة سرية، ويستوي أن تكون في مكان عام أو خاص، وكذلك التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص[2].

فعندما يتعلق الأمر بشأن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات فضابط الشرطة القضائية له سلطة اعتراض المراسلات التي تتم عبر وسائل الاتصال بنوعيها سلكية أو للاسلكية، ووضع الترتيبات التقنية دون موافقة الأشخاص المعنين بغرض التقاط وتثبيت وبث وتسجيل الأصوات المتفوه بها بصفة خاصة أو سرية من طرف الأشخاص سواء في مكان عام أو خاص، أو التقاط صور لأي شخص في أي مكان خاص، متى اقتضت ضرورات التحري ذلك، وهذا بموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري[3]، فيكون ذلك أثناء مرحلة التحريات الأولية التي تجريها الضبطية القضائية، أما خلال مرحلة التحقيق الإبتدائي، فإنه يمكن لقاضي التحقيق اللجوء لهذه الإجراءات من خلال

[1] عبد الرحمان خلفي، المرجع السابق، ص 142.

[2] حزيط محمد، الإختصاصات الإستثنائية المخولة لجهات المتابعة والتحقيق بشأن جرائم الفساد في القانون الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 05، العدد 02، 2020، ص367.

[3] محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، المرجع السابق، ص 208.

إذنه لضابط الشرطة القضائية الذي ينيبه وتحت رقابته، بنفس الشروط والكيفيات المنصوص عليها في مرحلة التحريات الأولية[1].

أ_ شروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

نظرا لخطورة هذه الإجراءات ومساسها بالحياة الخاصة، لذلك فالمشرع حرص على وضع شروط قانونية بهدف منع التعسف في استعمالها، وتتمثل هذه الشروط في:

_ الشروط الموضوعية لإعتراض المراسلات وتسجيل الأصوات والتقاط الصور: ويتمثل أهم شرط موضوعي في نوع الجريمة، حيث يشترط أن تكون الجريمة من بين الجرائم التي حصرها المشرع الجزائري في المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري، والتي من بينها هذا الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والشرط الثاني يتمثل في أن تكون هذه العمليات هامة وضرورية في مرحلة البحث والتحري عن الجريمة في حالة التلبس أو بمناسبة التحقيق، أما بالنسبة للشخص محل هذه العملية فلم يحدده المشرع فيمكن أن تُطبق على أي شخص يكون مشتبها فيه أو شاهد عن الجريمة، فالمبرر المقبول هو الضرورة التي تخضع لتقدير القاضي الآمر بالقيام بالعملية[2].

_ الشروط الشكلية لإعتراض المراسلات وتسجيل الأصوات والتقاط الصور: نصت على هذه الشروط المادة 65 مكرر5 من قانون الإجراءات الجزائية، فتتمثل هذه الشروط الشكلية في ضرورة الحصول على إذن كتابي من وكيل الجمهورية أو قاضي التحقيق، لمدة أقصاها 4 أشهر، قابلة للتجديد حسب ما يقتضيه البحث والتحري أو التحقيق[3]، وما يجدر بنا الإشارة إليه أن المشرع جعل المجال مفتوح للتجديد، ولم يحدد عدد المرات التي يمكن فيها القيام

[1] حزيط محمد، الإختصاصات الإستثنائية المخولة لجهات المتابعة والتحقيق بشأن جرائم الفساد في القانون الجزائري، المرجع السابق، ص 367.

[2] عبد الرحمان خلفي، المرجع السابق، ص 146.

[3] الطيب بلواضح، المرجع السابق، ص 183.

بتجديد الإذن[1]، ويكون هذا الأخير وفقًا لنفس الشروط الشكلية والزمنية[2] ويجب أن يتضمن جميع البيانات اللازمة التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة سواء كانت سكنية أم خلاف ذلك[3]، هذا ما نصت عليه المادة 65 مكرر 7 من قانون الإجراءات الجزائية الجزائري، والمشرع الجزائري لم يشترط في هذا الإذن شكلا معينا، وإنما تطلب فيه أن يكون مكتوبا، ويحتوي كذلك اسم الجريمة التي يؤسس عليها اللجوء لهذا الإجراء[4] وما يجدر الإشارة إليه أنه يجب على ضابط الشرطة القضائية أن يحرر محضر عن كل إجراء من الإجراءات السابق ذكرها، ويقوم بتحديد تاريخ بدايته والانتهاء منه في هذا المحضر[5]، وما يلاحظ على نص المادة السابق ذكره أنها تطلبت الإذن في تدبير اعتراض المراسلات المطلوب التقاطها دون التسجيل الصوتي أو الفيديو، وكذلك أن المشرع لم ينص على أي جزاء يترتب على عدم تطبيق أحكام هذه المادة، رغم أنه بدأها بالالزام من خلال استعماله لعبارة " يجب"[6].

ب_ كيفية اعتراض المراسلات في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

بخصوص اعتراض المراسلات، فإن هذه العملية يكون محلها عادة البريد الإلكتروني، والذي يعتبر من أهم وسائل الاتصال الحديثة في مجال الأنترنت، فهو بمثابة نظام ارسال عبر شبكة الانترنت، لأنه يحتوي على الكثير من المعلومات مثل تاريخ انشاء وارسال واستلام الرسالة، وعنوان كلا من المرسل والمستلم، ولكن المعلومات الواردة في تذييل رسالة البريد الالكتروني أهم من سابقتها، لأنها تحتوي على عنوان التعريف للمرسل، الذي يتكون

[1] عبد الرحمان خلفي، المرجع السابق، ص 147.

[2] أنظر الفقرة الأخيرة من المادة 65 مكرر 7 من ق.إ.ج.ج.

[3] الطيب بلواضح، المرجع السابق، ص 183.

[4] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010، ص 241.

[5] عبد الرحمان خلفي، المرجع نفسه، ص 147.

[6] فوزي عمارة، المرجع نفسه، ص 241.

من 4 أجزاء، في جزئه الأول من اليسار يبين المنطقة الجغرافية، و في الثاني مزود الخدمة والثالث مجموع الحاسبات الآلية المترابطة أما الجزء الأخير (الرابع) يحدد الحاسب الآلي الذي تم الاتصال منه[1].

2 _ إجراء التسرب:

عرفته المادة 65 مكرر 12 من قانون الإجراءات الجزائية في فقرتها الأولى بأنه "قيام ضابط أو أعوان الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق عملية العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خافٍ"[2].

أ_ شروطه التسرب:

_ الشروط الموضوعية للتسرب: تشير المادة 65 مكرر11 من قانون الاجراءات الجزائية الجزائري إلى شرط الضرورة بنصها "عندما تقتضي ضرورات التحري والتحقيق..."، وهذا الشرط ليس مطلق وانما مقيد بنوع الجريمة، حيث يجب أن تكون من الجرائم المحددة في المادة 65 مكرر5 ق.إ.ج.ج، والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات هذا من جهة، ومن جهة أخرى مرتبطة بالاستعجال المحصور في التلبس والتحقيق، والشرط الثاني يتمثل في اللجوء إليه احتياطيا أي يتم اللجوء إليه فقط عندما تكون وسائل التحري العادية غير كافية وهذا بهدف تجنب المساس بالحقوق، فيُلجأ إليه استثناء وبشروط محددة تحديد دقيق وبتوفير ضمانات كافية، أما الشرط الثالث وهو الملائمة حيث يُلجأ فقط لتسرب عندما يكون هناك اشتباه ضد أشخاص معينين بأنهم ارتكبوا جناية أو جنحة أو ربما هم على وشك القيام بها، أي وجود قرائن قوية هذا وفقًا للمادة 65 مكرر 12

[1] الطيب بلواضح، المرجع السابق، ص 184.

[2] أنظر المادة 65 مكرر 12 من ق.إ.ج.ج.

ق.إ.ج.ج، مع ضرورة التقيد بنوع الجريمة والتي تتمثل في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في دراستنا هذه[1].

ـ الشروط الإجرائية للتسرب: حددت المادة 65 مكرر 15 ق.إ.ج.ج الشروط الواجب توافرها في الإذن الممنوح بغرض القيام بعملية التسرب، حيث أوجبت أن يكون الإذن المسلم من طرف وكيل الجمهورية أو قاضي التحقيق للقيام بعملية التسرب في شكل مكتوب ويتضمن أسباب مبررة، وإلا فإنه يكون باطل[2]، مدته أقصاها أربعة أشهر، تُجدد بنفس المدة المذكورة لمرة واحدة، حسب ما يتطلبه البحث والتحري بنفس الشروط الشكلية والموضوعية، إضافة إلى أنه يتم ذكر الجريمة في الإذن الممنوح لضابط الشرطة القضائية المبررة لعملية التسرب والمتمثلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ويتم ذكر فيه هوية ضابط الشرطة القضائية المسؤول والمشرف على عملية التسرب، أو هوية عون الشرطة القضائية الذي يقوم بمساعدته، وما يشار إليه هنا أنه يُمنع إظهار الهوية الحقيقة لأي من ضباط وأعوان في أي مرحلة من مراحل الإجراءات حسب نص المادة 65 مكرر 16[3]، ويجب أن يتصف عمل الضابط بالمشروعية[4].

ثم يقوم ضابط الشرطة القضائية عند الانتهاء من عملية التسرب المكلف بها بتحرير محضرا يدون فيه كافة مجرى هذه العملية من بدايتها إلى غاية نهايتها ويرسله إلى وكيل

[1] عبد الرحمان خلفي، المرجع السابق، ص 150-151.

[2] علي شملال، المستحدث في قانون الإجراءات الجزائية الجزائري، الكتاب الثاني التحقيق والمحاكمة، د.ط، دار هومه، الجزائر، د. س. ن، ص 70.

[3] عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، المرجع السابق، ص 367-368.

[4] يتصف عمل الضابط بالمشروعية، فالضابط في هذه الحالة يستعمل الحيلة والتستر بغرض ضبط الفاعلين والمساهمين معهم، فإذا اعتمد سبيل غير مشروع أصبح عمله باطلا وهذا ما أكدته المادة 65 مكرر 12 في فقرتها الثانية، بأن لا يتحول التسرب إلى تحريض على الجريمة. أنظر عبد الله اوهايبية، المرجع نفسه، ص 368.

الجمهورية أو قاضي التحقيق الذي منحه الإذن لإجراء هذه العملية[1]، وما يجدر ذكره أنه يمكن القاضي الذي منح الرخصة أن يوقف هذه العملية في أي وقت[2].

ثم يقوم بإيداع الرخصة الممنوحة له في ملف الإجراءات حسب المادة 65 مكرر 15 من ق.إ.ج.ج[3]، ثم يضع تقرير يشمل جميع جوانب هذه العملية بالتفصيل، ويذكر فيه الأسماء والأماكن بدقة والوسائل التي تم استعمالها، والأشياء ذات الصلة والكيفيات التي تم من خلالها تم إيهام الفاعلين ومخادعتهم[4].

ب_ كيفية التسرب في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

ويمكن إجراء عملية التسرب في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في الفضاء السيبراني، وهذا ما تبته غالبية التشريعات المقارنة، ما دامت جميع الشروط والقواعد الإجرائية الواجب توافرها في هذه العملية متوافرة، فالتسرب الإلكتروني يعتبر أكثر حماية للشخص المتسرب، وبالتالي فالمشرع الجزائري ليس بحاجة لاستحداث نصوص خاصة، فالنصوص الواردة في ق.إ.ج.ج من المادة 65 مكرر 11 وما يليها كافية في هذا الصدد[5]. إن إجراء التسرب في الجريمة المرتكبة في الفضاء السيبراني يتمثل في دخول ضابط أو عون الشرطة القضائية إلى العالم الرقمي، وذلك من خلال اختراقه لبعض لمواقع المحددة وفتح الثغرات الإلكترونية فيها، أو اختراقه للحسابات الالكترونية المفتوحة في مواقع التواصل الإجتماعي واشتراكه في محادثات غرف الدردشة بها والظهور بمظهر الفاعل مثلهم من

[1] أحسن بوسقيعة، التحقيق القضائي، الطبعة الثانية عشر، دار هومه، الجزائر، 2018، ص 131.

[2] أنظر المادة 65 مكرر 15 من القانون رقم 06-22 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[3] أحسن بوسقيعة، المرجع نفسه، ص 132.

[4] عبد الرحمان خلفي، المرجع السابق، ص 152.

[5] ناني لحسن، المرجع السابق، ص 73.

خلال ايهامهم أنه فاعل معهم أو شريك لهم، مستخدما أسماء أو صفات مستعارة، وذلك من أجل الحصول على معلومات مفيدة في إجراء التحقيق[1].

وما يجدر بنا الإشارة إليه في هذا الصدد أن المشرع الجزائري نص على إجراء التسرب في البيئية الرقمية وأطلق عليه تسمية "التسرب الإلكتروني" في القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحته وبالضبط في المادة 26 منه التي ورد فيها أنه "مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن وكيل الجمهورية أو قاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن، تحت رقابته، لضابط الشرطة القضائية، بالتسرب الإلكتروني إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر، قصد مراقبة الأشخاص المشتبه في ارتكابهم لجريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم أنه فاعل أصلي معهم أو شريك لهم..."[2]

أما الفقرة الأخيرة من المادة السالفة الذكر فإنها تتوافق مع ما نصت عليه الفقرة الأخيرة من المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري حيث تحظر على كل ضابط من ضباط الشرطة القضائية القائم بعملية التسرب القيام بأي فعل أو تصرف مهما كان شكله، يؤدي إلى تحريض المشتبه فيه أو يشكل تحرضا على ارتكاب الجريمة، وذلك بهدف الحصول على دليل ضدهم[3].

ومما سبق يستنتج أن التسرب الإلكتروني أو الافتراضي يكون محله البيئة الالكترونية الافتراضية ذات الطابع المعنوي وليس المادي، حيث يتسرب إليها ضابط الشرطة القضائية ويظهر فيها بمظهر المجرم المعلوماتي أو شريك للمجرم المعلوماتي، وذلك من خلال

[1] الطيب بلواضح، المرجع السابق، ص 186.

[2] أنظر المادة 26 من القانون رقم 20-05 المؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر.ج.ج، العدد 25، المؤرخة في 6 رمضان عام 1441هـ الموافق ل 29 أبريل سنة 2020.

[3] أنظر الفقرة الأخيرة من المادة 26 من القانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية والفقرة الأخيرة من المادة 65 مكرر 12 من ق.إ.ج.ج.

اعتماده على الأساليب والبرامج التي تمكنه من النفاذ لهذه البيئة والتي هي في الأصل لا يمكن غير أولئك المجرمين أو شركائهم الدخول إليها، فمعيار الاختلاف الجوهري بين التسرب العادي (التقليدي) والتسرب الالكتروني يتمثل في البيئية محل عملية التسرب. لأن التسرب العادي يتمثل في دخول ضابط الشرطة القضائية داخل الجماعة الإجرامية لإيهامهم أنه فاعل معهم أو شريك واقعيًا وليس افتراضيا، أما التسرب الإلكتروني يكون من خلال دخول ضابط الشرطة إلى نظام المعالجة الآلية للمعطيات أو نظام الاتصالات الإلكترونية، مما يعني أنه تسربه محله البيئة الافتراضية.

وما يلاحظ أن عدم نص المشرع على أحكام إجرائية خاصة بإجراء التسرب الإلكتروني للبحث والتحري عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات سواء في قانون الإجراءات الجزائية أو القوانين الخاصة لا يؤدي إلى بروز فراغ تشريعي في هذا الصدد كون قانون الإجراءات الجزائية الجزائري نص على التسرب التقليدي وأحكامه والتي يمكن تطبيقها على التسرب الإلكتروني، هذا ما نص عليه القانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحته حيث نص عليه كإجراء فقط وتم إرجاء تطبيق أحكامه وفقا للقواعد العامة في قانون الإجراءات الجزائية.

وبالتالي كان من المستحسن كذلك النص عليه في القانون 09-04 والرجوع إلى تطبيق أحكامه وفقا لما ورد في قانون الإجراءات الجزائية الجزائري، كون هذا الإجراء خطير وماس بالحياة الخاصة للأفراد، حتى تكون هناك شرعية إجرائية في تطبيقه.

الفرع الثاني: القواعد الإجرائية المستحدثة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات في القانون رقم 09- 04

وما يجدر ذكره ان ظهور الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أدى بالمقابل إلى ظهور نوع مستحدث من التفتيش، ينصب هذا التفتيش على المنظومات المعلوماتية. حيث أن هذا النوع من التفتيش يختلف عن التفتيش العادي كونه ينصب على الكيانات المنطقية على عكس التفتيش التقليدي الذي محله مادي وليس منطقي، يتم إجراؤه في بيئة معنوية رقمية يستوجب الكشف عنها آليات فنية وبشرية خاصة، نظرا للطبيعة الخاصة للمعطيات الرقمية المخزنة إلكترونيا والمتمثلة في نبضات الكترونية، ويكون من خلال اتباع أليات مستحدثة لمعرفة الرقم السري (code)، أو كلمة السر(passwords)، أو نظام التشفير أو ترميز البيانات للوصول إلى مختلف الملفات[1].

أولا: إجراء تفتيش المنظومات المعلوماتية

1_تعريف تفتيش المنظومات المعلوماتية:

التفتيش في اللغة اسم، مصدره فتَّشَ، فتَّشَ على، فتَّشَ عن، فتَّشَ في، والتَّفتيش هو بحث السُّلطة في مكان معيّن، أثناء التَّحقيق القضائيّ، للعثور على ما يفيد الكشف عن الحقيقة[2].

أما فقها تم تعريفه من قِبل الفقه بأنه "إطلاع على البيانات المخزنة في النظام المعلوماتي"، وهناك من عرفه بأنه "إجراء ينصب على المعلومات ويسمح بجمع الأدلة

[1] يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، التواصل في الاقتصاد والادارة والقانون، جامعة باجي مختار عنابة، الجزائر، العدد 48، ديسمبر 2016، ص85.

[2] معجم المعاني الجامع- معجم عربي عربي، متوفر على الرابط التالي: https://www.almaany.com/ar/dict/ar-ar/%D8%AA%D9%81%D8%AA%D9%8A%D8%B4 تم الإطلاع عليه بتاريخ 2023/01/05 على الساعة 11:02.

المخزنة أو المسجلة في شكل إلكتروني"وعرف كذلك بأنه "كل ولوج إلى نظام معلوماتي من قبل السلطة هو بمثابة تفتيش إلكتروني باستثناء بعض الحالات المنصوص عليها"[1].

أما قانونا نصت عليه اتفاقية بودابست وأطلقت عليه تسمية "**تفتيش النظم المعلوماتية**" وعرفته في المادة 18 منها "تفتيش النظم المعلوماتية يقصد به البحث عن طريق التفتيش والضبط عن البيانات والمعطيات الإلكترونية المخزنة في النظام المعلوماتي للحاسب الآلي أو في دعامة تخزين المعلومات سواء كانت هذه البيانات مخزنة في جهاز واحد أو في منظومة اتصالات"[2].

ولم يُعرف المشرع الجزائري تفتيش المنظومات المعلوماتية وإنما ترك تعريفه للفقه. وبخصوص التفتيش المعلوماتي أو الإلكتروني كما يصطلح عليه، فإن المشرع الجزائري اصطلح عليه "**تسمية تفتيش المنظومة المعلوماتية**"، حيث جاء الفصل الثالث من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها موسوم ب " القواعد الإجرائية تفتيش المنظومات المعلوماتية"

ما يلاحظ أن غالبية تعريفات التفتيش الالكتروني أخذت بالتعريف التقليدي للتفتيش مع مراعاة أهم خصوصية البيئة التي يكون فيها هذا التفتيش المستحدث.

وأن ما يميزه هو أنه ينصب على الوسائل الإلكترونية[3]، وبالضبط على العناصر المنطقية، هذا وتجدر الاشارة هنا أن غالبية التشريعات اعتبرت مجرد الولوج إلى نظام

[1] رابح لهوى، الإشكاليات العملية الهامة للتفتيش الإلكتروني –دراسة مقارنة– الجزء الأول: إشكالية المفهوم والتكييف، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 06، العدد 02، 2020، ص 1224.

[2] Art 18 de la Convention sur la cybercriminalité.

[3] ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل الالكتروني في التشريع الجزائي الأردني، دراسات: علوم الشريعة والقانون، الجامعة الأردنية عمادة البحث العلمي، الأردن، المجلد 45، العدد 4، ملحق 2، 31 ديسمبر/ كانون الأول 2018، ص60.

المعالجة الآلية تفتيشا[1]، ففي الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات ففي الحالة التي يتم فيها نسخ نسخة من معطيات الحاسوب الموجودة في الملفات بواسطة برامج، فإنه لا يتم الكشف عن محتوى الملف المنسوخ بالكامل، وإنما سيكشف المفتش فقط على عبارات معينة وبالتالي يتم تحديد الملف على أنه يرجح استعماله كدليل رقمي، ويعرف القائم بعملية التفتيش محتواه الفعلي فقط عندما يفتح الملف ويطلع على المعطيات المتواجدة به[2]، ولكن بمجرد إجراء ضابط الشرطة القضائية بحثا عن الملف بالكلمة الرئيسة عن ملف يحتوي معطيات وبالتالي يعتبر هذا الإجراء تفتيشا بالرغم من الضابط لا يرى محتويات الملفات[3].

أما تفتيش المنظومات المعلوماتية عن بعد: لم يعرف المشرع الجزائري هذا النوع من التفتيش وإنما نص عليه فقط.

وحسب رأي الباحثة التفتيش عن بعد هو تفتيش معلوماتي لكن المفتش فيه يقوم بعملية التفتيش في الكيانات المنطقية عن بعد باستخدام الأنترنت ولا يكون قريب للحاسوب أو الجهاز الالكتروني محل التفتيش مثل التفتيش المعلوماتي العادي الذي يكون فيه أمام الحاسوب أي المكون المادي ومن خلاله يتم ولوجه إلى المكونات المنطقية ويقوم بتفتيشها. ويكون التفتيش عن بعد في هذه الاحتمالات الثلاثة:

_ اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان أخر داخل الدولة

_ اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان أخر خارج الدولة.

[1] لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، ، الجزائر، 2020- 2021، ص 102.

[2] Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 39, (2002), P107.

[3] Susan W. Brenner & Barbara A. Frederiksen, Ibid , P109.

_ التصنت والمراقبة الالكترونية لشبكات الحاسب[1].

2_ شروط تفتيش المنظومات المعلوماتية:

أ_ الشروط الموضوعية:

_ سبب لتفتيش تفتيش المنظومات المعلوماتية: للقيام بإجراء تفتيش المنظومة المعلوماتية لابد من وقوع جريمة من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، لأن الهدف الأساسي منه هو تحصيل أدلة رقمية تكشف الواقعة المُجَرّمَةِ[2]، إلا أن المشرع الجزائري في المادة 05 من القانون 09-04 أجاز التفتيش كإجراء وقائي كما سبق التطرق إليه[3]، ولا بد كذلك من وجود مشتبه فيه أو متهم بارتكاب الجريمة أو مشارك فيها[4].

_ محل التفتيش والجهة المختصة به: ويتمثل محل التفتيش المعلوماتي في البيئة الرقمية، لجهاز الحاسوب أو أي جهاز ذكي بمختلف مكوناته وشبكاته[5]، أما بخصوص الجهات المختصة بالتفتيش في هذه الجريمة فتتمثل في جهة التحقيق أو رجال الضبط القضائي[6]، المادة 05 من القانون 09-04.

[1] عبد الصبور عبد القوي علي المصري، منال عبد اللاه عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، ط 1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 1433هـ/ 2012، ص 302-304.

[2] إلهام بن خليفة، التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، المجلة القانونية للبحوث القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 2، العدد 1، 2018، ص32.

[3] إدريس قرفي، تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية: بين إتفاقية بودابست والتشريع الجزائري، مجلة الحقوق والحريات، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2014، ص 105-106.

[4] رجاء أومدور، التفتيش الجزائي في البيئة الإفتراضية، مجلة صوت القانون، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد07، العدد 01، ماي 2020، ص 978.

[5] رجاء أومدور، المرجع نفسه، ص 979.

[6] مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية- جامعة محمد خيضر بسكرة، العدد 22، جوان 2011، ص 238.

ب_ الشروط الشكلية:

لم ينص القانون رقم 09- 04 على الشروط الشكلية، وإنما أحال ذلك للقواعد العامة الواردة في قانون الإجراءات الجزائية الجزائري، وتتمثل هذه الشروط الشكلية في إصدار إذن بالتفتيش، حضور أشخاص محددين، والميعاد الزمني للتفتيش _سبق التطرق إليهم_

3 _إجراءات تفتيش مسرح الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

أ_ الإجراءات التقنية الأولية (القبلية) لعملية تفتيش المسرح الإفتراضي:

هناك مجموعة من القواعد الأساسية لا يجب الخروج عنها خلال مرحلة التفتيش، لاعتبارها ضرورية ومفيدة لتتبع الأدلة، كما أنها تحمي عملية التفتيش من أي طعن وتتمثل في منع تغيير الدليل الرقمي الأصلي، عدم تنفيذ وتطبيق البرامج المستخدمة في عملية التفتيش على الحاسوب أو الجهاز الذكي المتواجد في مسرح الجريمة، وحظر تعامل المشتبه فيه مع هذا الجهاز، مع الإحتفاظ بنسخة احتياطية عن الوسائط الرقمية المخزنة بها المعلومات والتي تم إيجادها في مسرح الجريمة، وتدوين جميع نشاطات التحقيق في محاضر، والاحتفاظ بالدليل الرقمي[1].

وأول إجراء قبلي لعملية التفتيش يتمثل في التخطيط حيث أنه وقبل بداية عملية التفتيش وقبل وصول القائمين بها إلى مسرح الجريمة يجب وضع خطة شاملة ودقيقة، حيث يجب في البداية على القائمين بعملية التفتيش أن يكونوا على معرفة ودراية تامة بإشكالات

[1] ناني لحسن، المرجع السابق، ص108 – 109.

الأدلة الرقمية وأساليب التعامل معها، من خلال تدريبهم على ذلك[1]. وتبيان مهام طاقم التفتيش وكل ما يتعلق بها من واجباتهم وسلامتهم وأمنهم[2].

ب_ الإجراءات التي يتم تنفيذها في مسرح الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات:

_ الإجراءات الأولى: وتتمثل في إغلاق أو تجميد مسرح الجريمة فهذا الإجراء بهدف حماية مسرحها بعدم حذف وإتلاف الأدلة الرقمية وفقدانها، والحرص على تأمينها وعدم المساس بمضامينها[3].

_ الإجراءات التالية التي ينبغي للفريق القيام بها: بداية يتم توثيق حالة مسرح الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات، من خلال تسجيل جميع تفاصيل الجهاز المستخدم في الجريمة أي كان نوعه (حاسب آلي، لوحة إلكترونية، هاتف ذكي...)، فيتم تحديد وضعه وقت ضبطه ما إذا كان في حالة تشغيل أم لا، أو متصل بالأنترنت أم لا، ثم يتم تحديد الجهاز المستخدم في الجريمة ومختلف الأجهزة المرفقة به الموجودة في مسرح الجريمة، ومن خلال رمز بروتوكول الانترنت (ip) يتم تحديد موقع ومكان المشتبه به المعلوماتي، ويتم كذلك تحديد وتوثيق أجهزة التخزين مثل الأقراص المضغوطة CDs وأقراص DVDs التي عُثر عليها، ويتم تصوير المسرح المادي وحفظ الأدلة بأنواعيها مادية

[1] سامر سلمان الجبوري، جريمة الاحتيال الإلكتروني دراسة مقارنة، الطبعة الأولى، منشورات زين الحقوقية، 2018، ص 155- 157.

[2] حيث يتم اعداد المهام الأساسية لطاقم التفتيش قبل الوصول إلى مسرح الجريمة إذا أمكن، ويؤخذ بعين الإعتبار أمن وسلامة وراحة طاقم التفتيش عند مواجهة مسرح الجريمة خاصة في الحالة التي يكون فيها هذا المسرح خطير، وتتم مناقشة التفتيش مع المشتركين فيه قبل الوصول إلى مسرح الجريمة إذا أمكن، ثم يتم اعداد الوسائل اللازمة للقيام 'بتوثيق التفتيش، وتقييم كل من مهام الطاقم المطلوبة لمعالجة مسرح الجريمة بشكل ناجح، والنتائج القانونية لتفتيش مسرح جريمة الحاسوب. أنظر ناني لحسن، المرجع السابق، ص108- 109.

[3] مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات، علوم الشريعة والقانون، المجلد 45، العدد4، ملحق 2، 2018، ص 286.

أو رقمية، والوثائق الورقية المطبوعة والأجهزة، وإجراء إسترجاع الوثائق المحذوفة، ونقل الأدلة المضبوطة[1]، من أجهزة ووسائط رقمية وأدوات، والحرص عليها أثناء نقلها، ويستحسن نقل القائم بالتفتيش بنفسه الأدلة إلى المخبر[2].

5 _ تمديد تفتيش المنظومات المعلوماتية:

أ_ تمديد تفتيش المنظومة المعلوماتية داخل الاقليم الوطني: إذا ما كان هناك شك بأن المعطيات الرقمية محل البحث الموجودة في منظومة معلوماتية أولى لها ارتباط بمنظومة ثانية، وتكون هناك إمكانية الدخول لها بواسطة الأولى، ففي هذه الحالة يصبح بالإمكان تمديد التفتيش إلى كل المنظومة الثانية أو جزء منها، وذلك شريطة إعلام الجهة القضائية المختصة[3].

ب_ تمديد تفتيش المنظومة المعلوماتية خارج الإقليم الوطني: وفي حالة تواجد هذه المعطيات محل البحث في منظومة معلوماتية أجنبية، فإنه يتطلب الحصول عليها من خلال المساعدة المقدمة من طرف السلطات الأجنبية لتلك الدولة، بما يتلائم والاتفاقيات الدولية في هذا الشأن، ومبدأ المعاملة بالمثل. ويجوز استدعاء أي شخص له علم كاف بأساليب عمل المنظومة المعلوماتية محل البحث أو بإجراءات حماية المعطيات المعلوماتية التي تحتويها هذه المنظومة من قِبل السلطات القائمة بعملية التفتيش، وذلك بغية مساعدتهم في إنجاز المهمة الموكلة لهم، وتقديم كل المعلومات الكافية[4].

[1] مصطفى عبد الباقي، المرجع السابق، ص 286.

[2] سامر سلمان الجبوري، المرجع السابق، ص 164.

[3] أنظر المادة 05 من القانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4] أنظر المادة 05 من القانون رقم 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ثانيا: الحجز

1_ الحجز الكلي للمنظومة المعلوماتية:

الأصل هو الحجز الكلي للمنظومة المعلوماتية[1]، وكما معلم أنه لا يكون الحجز إلا على الأشياء المادية الملموسة، ففي الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تتمثل مثلا في الأدلة المادية الموجودة على المكونات المادية للكمبيوتر، مثل رفع بصمات الأصابع، وضبط الدعامة المادية للبرامج المستعملة، لكن الإشكال يُثار إذا ما تعلق الأمر بضبط المعطيات والمكونات المنطقية[2]، وفي هذا الصدد ظهر إتجاهيين فقهيين حول إمكانية الحجز على المنظومة المعلوماتية وبياناتها المنطقية: الاتجاه الأول يقول بعدم إمكانية تصور إجراء الحجز على الكيانات المنطقية وذلك لغياب الكيان المادي[3]، الذي يجعلها محلاً للحجز، وعليه لا يمكن القيام به إلا بعد نقلها على كيان مادي، من خلال تصويرها فوتوغرافيا، أو بنقلها على وسائط مادية مثلا، أما الإتجاه الثاني يقول بأن المعطيات المعالجة إلكترونيا تتمثل في ذبذبات إلكترونية أو موجات كهرومغناطيسية، يمكن تسجيلها وحفظها وتخزينها، لذا لا يمكن إنكار وجودها المادي[4].

2 _ الحجز الجزئي للمنظومة المعلوماتية:

فالأثر المباشر لعملية التفتيش وهو النسخ، والإشكال الذي يُثار هنا ما هو التكييف القانوني لعملية النسخ؟ وهل النسخ الإلكتروني يعتبر حجزا في الحالة التي يتم فيها إبقاء الأجهزة المادية بحوزة المتهم؟ والمشرع الجزائري في هذا الصدد حل هذا الإشكال من خلال

---

[1] المنظومة المعلوماتية عرفتها المادة 2 من القانون 09-04 بأنها "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، مصر، 2009، ص 274.

[3] الطيب بلواضح، المرجع السابق، ص 160.

[4] خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، المرجع السابق، ص 119.

نصه بأنه عندما يتم إكتشاف السلطة القائمة بالتفتيش معطيات ضمن منظومة معلوماتية، وتكون هذه الأخيرة مفيدة للكشف عن الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات أو المجرمين المعلوماتيين، ويكون ليس محتومًا حجز المنظومة ككل، فإنه "**يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز**"، ويكون ذلك وفقا للقواعد التي نص عليها قانون الإجراءات الجزائية الجزائري[1]، وهو نفس ما سار عليه المشرع الفرنسي[2].

أ_ الأساس الفقهي لتكييف نسخ المعطيات بأنه حجز:

اعتمد الفقه ثلاثة معايير لتكييف نسخ المعطيات بأنه ضبط تتمثل فيما يلي: المعيار1: أن النسخ الرقمي للمعطيات يتعارض مع الحق في حذف المعطيات وهذا الحق سبق التعرض له، وبالتالي فإن نسخ هذه المعطيات يعتبر حجزا، المعيار2: النسخ الرقمي للمعطيات يتعارض مع الحق في الحيازة الحصرية للمعلومات: فعندما تقوم الجهة المختصة بعملية نسخ المعطيات التي لم تكن في حيازتها، فإن تحرم صاحبها من حق استعمال المعطيات بشكل فردي، ويصبح لا يستطيع التمتع بحقه في استبعاد الغير عنها[3].

المعيار3: هذا الرأي يرى أن نسخ المعطيات حجزًا باعتبار أن لهما نفس الهدف المتمثل في التحكم في مسرح الجريمة والأدلة الرقمية التي يتضمنها، والأمر ذاته بخصوص إنشاء نسخة إلكترونية من المعطيات الذي يُجمد المعطيات ليتم استعمالها كدليل رقمي[4].

---

[1] أنظر المادة 06 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2] الذي نص على عملية نسخ المعلومات والمعطيات التي تنتج عن التفتيش على دعامات التخزين الإلكترونية وتحريزها وهذا وفقا للتعديل الذي طرأ على ق.إ.ج.ف من خلال القانون رقم 2003/239 استحدث الفقرة الثالثة من المادة 57. أنظر الطيب بلواضح، المرجع نفسه، ص 160- 161.

[3] هذا حسب تفسير القضاء الامريكي الدائرة الاستئنافية الفيدرالية الثانية في قضية States v.Ganias United.

[4] لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، المرجع السابق، ص 93- 96.

وعليه فإن النسخ الرقمي لمعطيات المتهم يشكل "**حجزا**"، لأن إنشاء نسخة إلكترونية لا يختلف عن عملية إجراء حجز الأشياء المادية، الذي من خلاله سلطة التحقيق تضمن السيطرة على الشيء الذي يحتمل استخدامه كدليل رقمي له قيمة في الإثبات[1].

ومن الناحية العملية يتم نسخ المعطيات المطلوبة في إجراءات البحث والتحري والمحتواة في نظام المعالجة الآلية للمعطيات، لتفتيشها لاحقا، لأن الأجهزة المادية والنسخة الأصلية للمعطيات تبقى لدى المتهم في وعائها المادي المتمثل في وسيط التخزين الإلكتروني، وهذا مرده تجنب الأضرار التي قد تمس الأفراد والمؤسسات لاسيما الإقتصادية منها الناجمة عن عرقلة نشاطها، عند حجز الأجهزة المادية الخاصة بها بمحتواها المنطقي[2]، لأنه عمليا يصعب الفصل بين وسيط التخزين الالكتروني والمعطيات إلا من خلال نسخ هذه المعطيات في وعاء مادي أخر. فالمحقق من خلال عملية تفتيش الحواسيب يجدها تحتوي عدد هائل من الملفات، فغربلتها والبحث عن الملفات التي تحتوي على معطيات تشكل دليلا رقمي قد يستغرق وقتا طويلا، لذا فغالبا ما يأخذون نسخة من هذه الملفات التي تحتوي على معطيات ثم يقومون بتحليلها لاحقا[3].

ب_ أشكال الحجز الجزئي للمعطيات:

_ حجز المعطيات اللازمة لفهم المعطيات المحجوزة: هناك حالات يكون فيها حجز المعطيات ذات المحتوى المجرم التي ستكون بمثابة دليل رقمي غير كافٍ إذا لم يكون مصحوبًا بحجز المعطيات اللازمة لفهمها، ومن أمثلة ذلك الحالة التي يتم فيها متابعة شخص قام بنشره صور أو منشورات ذات محتوى مجرم على مواقع التواصل الاجتماعي

[1] رابح لهوى، الإشكاليات العملية الهامة للتفتيش الإلكتروني –دراسة مقارنة– الجزء الأول: إشكالية المفهوم والتكييف، المرجع السابق، ص 1228.

[2] رابح لهوى، الإشكاليات العملية الهامة للتفتيش الإلكتروني –دراسة مقارنة– الجزء الأول: إشكالية المفهوم والتكييف، المرجع نفسه، ص 1228.

[3] Orin S. Kerr, Fourth Amendment Seizures of Computer Data, Yale Law Journal, Vol. 119, Issue 4, (2010), p 704.

كالفايسبوك (facebook)، فهنا لا يكفي نسخ المحتوى الإجرامي وحجزه وحده، بل يستوجب نسخ الصفحة بالكامل وبشكل تفاعلي، بصيغة HTML [1]، وليس مجرد تصويرها، وذلك بغرض إثبات واقعة النشر المُجَرم، ومعرفتة طريقتها، كون الطرق تتعدد فهناك منها النشر المفتوح للعامة، والنشر المحدد لأشخاص معينين، ويتم معرفة نوعه من خلال الصيغة التفاعلية المحجوزة، لأنه يصبح ذلك مستحيلاً إذا تم الاكتفاء بالصور فقط دون حجز الصيغة كاملة، كما أنه يمكن أن يكون الملف ذو المحتوى المجرم غير منشور، لذا فإن عملية حجز المعطيات المساعدة لفهم المعطيات المحجوزة الأساسية، يُعطي حجية أكثر للدليل الرقمي المتحصل عليه منها، إضافة إلى أنه يساعد جهات الحكم في فهم وتحليل المشكلات الفنية والتقنية وبالتالي الوصول إلى حكم عادل[2].

_حجز المعطيات ذات المحتوى المجرم: مكنت المادة 8 من نفس القانون السلطة القائمة بعملية التفتيش من الأمر بإتخاذ الإجراءات الضرورية بغرض منع الإطلاع على المعطيات التي يشكل مضمونها جريمة، من خلال الطرق اللازمة خاصة من خلال تكليف المؤهلين تقنينا باستخدام الطرق والتقنيات المناسبة لذلك[3]. ويلاحظ أن هذه الطريقة المتمثل في تكليف شخص مؤهل وردة على سبيل المثال وليس على سبيل الحصر، هذا ما يستشف من العبارة التي إستعملها المشرع وهي عبارة "لاسيما" التي تفيد الترجيح.

---

[1] **HyperText Markup Language** باللغة العربية هي لغة ترميز النص الفائق: هي لغة ترميز تستخدم في إنشاء وتصميم صفحات ومواقع الويب، وتعتبر هذه اللّغة من أقدم اللّغات وأوسعها استخداما في تصميم صفحات الويب . HTMLهيكل صفحة الويب وتعطي متصفّح الإنترنت وصفا لكيفيّة عرضه لمحتوياتها. موسوعة ويكيبيديا، متوفر على الرابط التالي:
https://ar.wikipedia.org/wiki/%D9%84%D8%BA%D8%A9_%D8%AA%D9%88%D8%B5%D9%8A%D9%81_%D8%A7%D9%84%D9%86%D8%B5_%D8%A7%D9%84%D9%81%D8%A7%D8%A6%D9%82
تم الإطلاع عليه بتاريخ: 05/16/ 2023 على الساعة 07:53.

[2] ناني لحسن، المرجع السابق، ص 122 – 123.

[3] أنظر المادة 08 من من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وفي المقابل مكنت بعض التشريعات المقارنة كالمشرع الفرنسي كل من وكيل الجمهورية أو قاضي التحقيق من الحذف النهائي للمعطيات المجرمة من الوسائط الأصلية التي تهدد الأشخاص في أمنهم وممتلكاتهم وحياتهم الخاصة مثل الإعتداء الجنسي على الأطفال[1].

ـ الحجز عن طريق المنع للوصول: هذا الإجراء نصت عليه المادة 07 من القانون 09-04، فللقيام بالحجز عن طريق المنع للوصل يتوجب توافر شرط إستحالة الحجز، الذي مرده أسباب تقنية، ففي هذه الحالة تمنع السلطات التي تقوم بإجراء التفتيش فيمنع الوصول إلى كل من المعطيات التي يتضمنها نظام المعالجة الآلية، أو إلى النسخ التي بحوزة الأشخاص المرخص لهم باستعماله[2]، فهذا الإجراء يعتبر وقائي واحترازي، الهدف المرجو منه هو الحفاظ على الأدلة الرقمية في بيئتها الرقمية الأصلية، وهذا يتلائم مع طبيعتها الخاصة التي تتميز بسرعة الطمس والاتلاف[3].

ج ـ حدود إستعمال المعطيات المحجوزة وكيفية التعامل معها في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات:

بعد القيام بأي عملية تفتيش أو **معاينة تقليدية أو إلكترونية[4]**، يتم استخراج نسخة من المعطيات المحجوزة على الدعائم الإلكترونية لجهة التحقيق أو الحكم، وذلك إذا لم يتم حجز المنظومة بكاملها، وتُترك تحت تصرفها إلى غاية إنتهاء المحاكمة، مع إمكانية تشكيل هذه

[1] Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, Droit pénal appliqué», 2010, ECONOMICA, Paris France, 2010 , p 179.

[2] أنظر المادة 07 من من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، العدد5 ، جوان 2012، ص177.

[4] هذا النوع من المعاينة يعتبر نوع مستحدث لأن الانتقال فيها لا يكون عبر العالم المادي وإنما يكون عبر العالم المعنوي إذ يمكن أن تكون عن طريق الشبكة المعلوماتية، فالقائم بالتحقيق (ضابط ش ق أو المحقق)، ينتقل إلى الفضاء الإلكتروني من خلال لجوئه إلى مقر عمل مزود بخدمة الانترنت، والذي من خلاله يقوم بإجراء المعاينة. أنظر لينا محمد الأسدي، المرجع السابق، ص 204.

المعطيات واعادة تشكيلها بواسطة الوسائل التقنية لجعلها تتناسب مع أهداف إجراء التحقيق شريطة عدم المساس بجوهر المعطيات[1]، المشرع لم يترك إستعمال هذه المعطيات المُحصلة مطلقًا وإنما أورد قيودًا على استعمالها لأن الحجز أحيانا يشكل مساسًا بالحقوق ولاسيما الحق في الخصوصية، وضمانا لإحترام هذه الحقوق أقر المشرع ضمانات من خلال فرضه لحدود إستعمال المعطيات[2]، المعطيات المحجوزة إلا بما يسمح به القانون، واستخدامها بالقدر الضروري الذي تتطلبه التحريات أو التحقيقات القضائية [3].

المطلب الثاني: إستحداث جهات قضائية متخصصة في المتابعة والتحقيق والمحاكمة في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات

إن خصوصية الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وتعقيدها وتشعبها وخطورتها جعل القضاء أو بالأحرى المحاكم ذات الاختصاص العادي عاجزة على مواجهتها والتصدي لها، وهذا مرده محدودية الإختصاص القضائي (الإختصاص القضائي المحلي ليس موسع)، خاصة أن هذه الجريمة تُرتكب على نطاق إقليمي واسع وعابر للحدود الوطنية، وكذلك عدم تخصص القضاة الناظرين في النزاع الذي محله جريمة من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات التي تشهد تطور مستمر وأساليب حديثة ومتجددة لارتكابها، ما جعل المجرمين المعلوماتيين باعتبارهم من أذكى المجرمين يتملصون من العقاب بسبب الدليل الرقمي سريع الضياع والمحو.

وبالتالي أصبح إنشاء جهات قضائية متخصصة ضرورة ملحة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وبإنشاء الأقطاب الجزائية أصبحت تتمتع بسلطة المتابعة والتحقيق والمحاكمة، وعليه من خلال هذا المطلب سنتطرق إلى القواعد الجزائية الإجرائية

[1] ناني لحسن، المرجع السابق، ص 124.

[2] ناني لحسن، المرجع نفسه، ص 125.

[3] أنظر المادة 09 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

التي نظمت الأقطاب الجزائية المتخصصة، والذي قسمناه إلى فرعين الفرع الأول معنون بالجهات القضائية ذات الاختصاص الموسع، أما الفرع الثاني المعنون بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

الفرع الأول: الجهات القضائية ذات الاختصاص الموسع

الأقطاب الجزائية المتخصصة أو كما أطلق عليها المشرع في قانون الإجراءات الجزائية الجزائري الجهات القضائية الموسعة، حيث تعتبر المحاكم ذات الاختصاص المحلي الموسع أقطابا جزائية متخصصة لها اختصاص إقليمي موسع[1]. وتتمتع الأقطاب الجزائية المتخصصة، بصلاحيات قضائية موسعة، في مجال الجرائم التي تتطلب كفاءة عالية وتقنيات تحري خاصة.

تُعرف الأقطاب الجزائية كذلك بأنها "محاكم عادية من الدرجة الأولى، وسع إختصاصها المحلي في إطار الوقاية من الظاهرة الإجرامية المستحدثة ومكافحتها، التي استفاد مرتكبوها من التطور العلمي والتكنولوجي فاستعملوه في إجرامهم"[2].

أولا: إختصاص الجهات القضائية ذات الاختصاص الموسع

1_ الإختصاص الإقليمي:

ويقصد به الحدود التي رسمها المشرع لقضاة النيابة أو التحقيق أو الحكم لممارسة اختصاصهم في الدعوى المعروضة عليهم، وقد بين قانون الإجراءات الجزائية في المواد 37 و40 و329 توسيع الإختصاص المحلي لكل منهم في الجرائم المتميزة بالخطورة والتعقيد[3] والتي حددها ومن بينها الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وحسب المرسوم

[1] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري- الجزء الثاني-، المرجع السابق، ص67.

[2] عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري- الجزء الثاني-، المرجع نفسه، ص 74.

[3] عبد الفتاح قادري، حيدرة سعدي، آليات عمل الأقطاب الجزائية المتخصصة في جرائم الفساد، مجلة العلوم الإنسانية لجامعة أم البواقي، جامعة العربي بن مهيدي، أم البواقي، الجزائر، المجلد8، العدد1، مارس 2021، ص200.

التنفيذي رقم 06- 348 المؤرخ في 10 اكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، حدود الاختصاص المحلي الجديد للمحاكم المعنية بهذا التوسع والمتمثلة في:

- القطب الجزائي لمحكمة سيدي امحمد بالجزائر[1] يغطي منطقة الوسط
- القطب الجزائي محكمة قسنطينة[2]، يغطي منطقة الوسط
- القطب الجزائي لمحكمة ورقلة[3] يغطي منطقة الجنوب
- القطب الجزائي محكمة وهران[4] يغطي منطقة الغرب

2_ الاختصاص النوعي:

تشمل فقط نوعا معين من الجرائم المحددة على سبيل الحصر في القانون، والتي تتمثل في دراستنا في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[1] انظر المادة الثانية من المرسوم التنفيذي رقم 16-267 مؤرخ في 15 محرم عام 1438 الموافق 17 أكتوبر سنة 2016 يعدل المرسوم التنفيذي رقم 06- 348 المؤرخ في 12 رمضان 1427 الموافق 5 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج العدد 62، مؤرخة في 21 محرم عام 1438 الموافق 23 أكتوبر سنة 2016.

[2] انظر المادة 3 من المرسوم التنفيذي رقم 16-267 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

[3] أنظر المادة 4 من المرسوم التنفيذي رقم 16-267 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

[4] أنظر المادة 5 من المرسوم التنفيذي رقم 16-267 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

ثانيا: كيفية إتصال قاضي الجهات القضائية ذات الاختصاص الموسع بملف الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات

1_ بالنسبة لاتصال وكيل الجمهورية بالمحكمة ذات الاختصاص الإقليمي الموسع:

نصت المادة 40 مكرر 1 من الأمر 20-04 المؤرخ في 30 غشت سنة 2020 أنه عندما يتعلق الأمر بإحدى الجرائم التي نص عليها قانون الإجراءات الجزائية في الفقرة الثانية من المادة 37[1]، والتي من بينها والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[2]، حيث يخبر ضابط الشرطة القضائية على الفور وكيل الجمهورية لدى المحكمة المختصة إقليميا وكما نعلم الإختصاص الإقليمي يتحدد بمكان ارتكاب الجريمة أو المكان الذي يقيم فيه المتهم أو المكان الذي ألقى فيه القبض عليه حسب المادة 37 إذا ما تعلق الأمر بوكيل الجمهورية، وهي نفس الضوابط التي يتحدد بها الإختصاص إذا تعلق الأمر بقاضي التحقيق وفقا للمادة 40 من ق.إ.ج.ج، وما يلاحظ أن المشرع حسنا فعل بتعديله للمادة 40 مكرر 1 عدل عبارة "المحكمة الكائن بها مكان الجريمة" بعبارة "المحكمة المختصة إقليميا" لأن المادة قبل تعديلها قصرت الإختصاص على مكان إرتكاب الجريمة دون مراعاة مكان الإقامة ومكان إلقاء القبض، وبالتالي فهنا يتم المساس بقاعدة من النظام العام مهمة وهي قاعدة عدم جواز الإتفاق على مخالفة قواعد الإختصاص في المادة الجزائية. فبعد قيام ضباط الشرطة القضائية بإخبار وكيل الجمهورية فورا لدى المحكمة المختصة إقليميا، يقومون بإرسال له الأصل ونستخين من إجراءات التحقيق، ثم يقوم وكيل الجمهورية لدى المحكمة

[1] أنظر المادة 40 مكرر 1 من الأمررقم 20-04 مؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 51 مؤرخة في 12محرم عام 1442، الموافق 31 غشت 2020.

[2] أنظر المادة 37 من القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج العدد 71، المؤرخة في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

المختصة إقليميا بإحالة فورا النسخة الثانية إلى وكيل الجمهورية لدى الجهة القضائية ذات الإختصاص الإقليمي الموسع[1] أي وكيل الجمهورية لدى القطب الجزائي المتخصص.

2_ بالنسبة لاتصال قاضي التحقيق بالمحكمة ذات الاختصاص الإقليمي الموسع:

يتم إتصال قاضي التحقيق بالمحكمة ذات الإختصاص الإقليمي الموسع أو القطب الجزائي المتخصص بالملف، وفقا للطريق العادي لتحريك الدعوى العمومية عن طريق الطلب الافتتاحي الصادر عن وكيل الجمهورية لتلك الجهة القضائية في الحالة التي يتوصل فيها مباشرة بمحاضر التحريات الأولية من الضبطية القضائية، أو بعد موفاته بملف الإجراءات إذا كان قد طالب به بعد أخذ رأي النائب العام إذا اعتبر أن الجريمة تدخل ضمن اختصاص القطب الجزائي المتخصص وفقا لما نصت عليه المادة 40 مكرر 2 من قانون الإجراءات الجزائية على ضوء تعديل قانون الإجراءات الجزائية في سنة 2020 بالأمر رقم 20-04، أما في الحالة التي يسبق فيها فتح تحقيق قضائي بالمحكمة الأصلية، فيتصل قاضي التحقيق بالملف بموجب أمر بالتخلي عن القضية يصدره قاضي التحقيق للمحكمة العادية لفائدة قاضي التحقيق بالقطب الجزائي المتخصص لدى المحكمة المختصة، وفقا لما جاء في المادة 40 مكرر3 من قانون الإجراءات الجزائية على ضوء التعديل 20-04 لسنة 2020.[2]

فبالنسبة للجرائم الخطيرة التي الواردة في الفقرة الثانية من المادة 37[3] بصفة عامة وجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بصفة خاصة والتي تمثل موضوع دراستنا فإنها لا تُثار مسألة الإختصاص، إلا إذا اعتبر وكيل الجمهورية لدى القطب الجزائي المتخصص أن الجريمة تدخل ضمن إختصاص القطب الجزائي المتخصص وطالب بملف

[1] أنظر المادة 40 من القانون رقم 04-14 المعدل والمتمم لقانون الإجراءات الجزائية.

[2] محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري على ضوء آخر التعديلات لقانون الإجراءات الجزائية والاجتهاد القضائي، الطبعة الثالثة، دار بلقيس، الدار البيضاء، الجزائر، 2022، ص 205.

[3] المادة 37 من القانون رقم 04-14 المعدل والمتمم لقانون الإجراءات الجزائية.

الإجراءات الخاصة بها، فالفقرة الأولى من المادة 40 مكرر3 تمنحه سلطة التمسك باختصاص هذه الجهة القضائية والمطالبة بملف الإجراءات خلال جميع مراحل الدعوى[1].

الفرع الثاني: إستحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

إستحدث المشرع الجزائري القطب الجزائي السيبراني المتخصص فقط في متابعة والتحقيق والمحاكمة في جرائم السيبرانية بمقتضى الأمر رقم 21- 11 المؤرخ في 25 غشت سنة 2021 المتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، تم النص على إنشاء القطب الجزائي السيبراني، حيث تُمم قانون الإجراءات الجزائية بباب سادس عُنون "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال"، وتضمن هذا الباب 8 مواد من المادة 211 مكرر 22 إلى المادة 211 مكرر 29.

فيُنشأ هذا القطب على مستوى محكمة مقر مجلس قضاء الجزائر أي بمحكمة سيدي محمد، وهذا القطب متخصص بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها، ويختص كذلك بالحكم في هذه الجرائم إذا كانت تشكل جُنحا[2].

من خلال قراءة الفقرة الأولى من المادة 211 مكرر 22 يتضح أن هذا القطب يختص بالمتابعة والتحقيق في جميع الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها سواء كان وصفها جنحة أو جناية، لأن المشرع لم يحدد نوع الجريمة التي يختص هذا القطب بمتابعتها والتحقيق فيها.

[1] محمد حزيط، المرجع السابق، ص 206.

[2] أنظر المادة 211 مكرر 22 من الأمر رقم 21- 11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج ، العدد 65 المؤرخة في 17 محرم عام 1443 هـ الموافق 26 غشت سنة 2021.

عكس ما ورد في المادة بالنسبة للحكم حيث يختص فقط في الجرائم التي توصف جنحا، دون الجنايات لأن نص المادة السالفة الذكر حدد ذلك، وبالتالي فإنه بعد المتابعة والتحقيق في الجريمة التي يكون وصفها جناية – وهذا عادة يكون بالنسبة للجرائم المرتبطة بالجرائم المتعلقة بتكنولوجيات الاعلام والاتصال، لأن جل جرائم المساس بأنظمة المعالجة الآلية البحتة، والجرائم المتعلقة بالمعطيات الشخصية جميعها أعطاها المشرع وصف الجنحة تماشيا مع سياسة التجنح المعمول بها– ، فإنه يتم إرسال مستندات القضية إلى محكمة الجنايات للفصل فيها.

والجرائم المتصلة بتكنولوجيات الإعلام والاتصال في الأمر 21–11 يقصد بها "أي جريمة تُرتكب أو يسهل إرتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والإتصال"[1]، وهذا التعريف شامل يتضمن كذلك الجرائم المساس بأنظمة المعالجة الآلية للمعطيات، وهي الجرائم التي يتم المساس فيها بالمنظومة المعلوماتية.

وهو نفس التعريف الوارد في المادة 2 القانون 09–04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن هذا التعريف تم ذكر فيه جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات خلافا لما ورد في الأمر المستحدث حيث ورد كما يلي "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية"[2].

[1] أنظر المادة 211 مكرر 22 من الأمر رقم 21–11 المتمم لقانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 02 من القانون 09–04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أولا: الأحكام المنظمة لقواعد إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال

1_ قواعد إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

أ_ الإختصاص الإقليمي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

نصت عليه المادة 211 مكرر 23 من الأمر رقم 21-11 "يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني" من خلال المادة السالفة الذكر يتضح أن للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال اختصاص إقليميا وطنيا، يمتد لكافة إقليم الدولة الجزائرية كوحدة إقليمية، هذا مرد خصوصية هذه الجرائم المستحدثة التي تتسع الرقعة الجغرافية التي تُرتكب فيها، وإختلاف مكان تواجد مرتكبيها وتتميز بالخطورة والتعقيد والتشعب[1].

ب_الإختصاص النوعي الحصري للقطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

يختص القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال نوعيًا وحصريًا بجرائم محددة.

[1] بن عمیور أمینة، بوحلایس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عدد خاص بفعاليات الملتقى الدولي: " القانون الجنائي للأعمال نحو توجه جديد للتجريم " المنعقد يوم 21 أكتوبر 2021 عبر التحاضر المرئي عن بعدZOOM، مجلة البحوث في العقود وقانون الأعمال، مخبر العقود وقانون الأعمال، جامعة الإخوة منتوري قسنطينة1، قسنطينة، الجزائر، المجلد 07، العدد 01، 2022، ص74.

ويقصد ب الإختصاص الحصري الاختصاص الذي ينفرد به القطب المستحدث دون سواه بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، ولا يمكن أن يشرك معه اي جهة قضائية جزائية أخرى مهما كان نوعها سواء كانت عادية أو قطب جزائي[1].

والإختصاص الحصري يكون في جنح محددة على سبيل الحصر:

وفقا لنص م211 مكرر 24 من ق.إ.ج.ج فإنه يختص هذا القطب المستحدث ب:

_ "بالجرائم التي ترتكب أو يسهل إرتكابها باستعمال منظومة معلوماتية أو نظام الاتصالات الالكترونية أو أي وسيلة أخرى آلية ذات صلة بتكنولوجيات الإعلام والاتصال"

_ " الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني

_ جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو إستقرار المجتمع

_ جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية،

_ جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية،

_ جرائم الإتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين،

_ جرائم التمييز وخطاب الكراهية"[2].

نصت المادة 211 مكرر 24 في هذه الجرائم يؤول الإختصاص لوكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال وقاضي

[1] شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس، المدية، الجزائر، المجلد08، العدد02، جوان 2022، ص493.

[2] أنظر المادة 211 مكرر 24 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

التحقيق ورئيس ذات القطب حصريا بالمتابعة والتحقيق والحكم في هذه الجرائم التي سبق ذكرها، والجرائم المرتبطة بها[1].

والإرتباط هنا لا يهم إن كان إرتباطا حقيقيا قابل للتجزئة، أو إرتباط صوري غير قابل للتجزئة، ولا يشترط لإنعقاد إختصاص القطب بشأن هذه الجرائم المرتبطة أن تكون مرتكبة هي الأخرى بإستعمال تكنولوجيات الإعلام والإتصال، وإنما يكتفي بالجريمة الأصلية التي يجب أن تتوفر على هذا الشرط الأساسي لتقرير الإختصاص[2].

والإرتباط نصت عليه المادة 188 من قانون الإجراءات الجزائية الجزائري حيث حددت الحالات التي تعتبر فيها الجرائم مرتبطة على سبيل الحصر[3].

أما الإختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال يقصد به أن تكون الجهة القضائية تختص بالنظر في هذا النوع من الجرائم يحدده القانون بحسب طبيعته أو جسامته[4]، وبالتالي فالاختصاص النوعي للمحاكم

[1] أنظر الفقرة 1 من المادة 211 مكرر 24 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[2] شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، المرجع السابق، ص 492.

[3] تنص المادة 188 من قانون الإجراءات الجزائية الجزائري على أنه: " تعد الجرائم مرتبطة في الأحوال الآتية:

أ) إذا إرتكبت في وقت واحد من عدة أشخاص مجتمعين،

ب) إذا إرتكبت من أشخاص مختلفين حتى ولو في أوقات متفرقة وفي أماكن مختلفة ولكن على إثر تدبير إجرامي سابق بينهم،

ج) إذا كان الجناة إرتكبوا بعض هذه الجرائم للحصول على وسائل ارتكاب الجرائم الأخرى أو تسهيل ارتكابها أو إتمام تنفيذها أو جعلهم في مأمن من العقاب،

د) أو عندما تكون الأشياء المنتزعة أو المختلسة أو المتحصلة عن جناية أو جنحة قد أخفيت كلها أو بعضها"

[4] بن عميور أمينة، بوحلايس إلهام، المرجع السابق، ص76.

يتحدد على أساس نوع الجريمة، وهذا الأخير يتحدد على أساس العقوبة المنصوص عليها في قانون العقوبات أو القوانين المكملة له[1].

وحسب نص المادة 211 مكرر22 فإن القطب يختص بنوع محدد من الجرائم كما سبق وأن ذكرنا والمتمثل في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، حيث يختص وكيل الجمهورية لدى القطب في مرحلة بمتابعة هذا النوع من الجرائم المستحدثة، وخلال مرحلة التحقيق يختص قاضي التحقيق لدى القطب المستحدث بالتحقيق فيها، ويختص قاضي الحكم بالنوع السابق الذكر من الجرائم إذا كانت تشكل جنحا فقط، وبالتالي فالجنايات تختص بها محكمة الجنايات[2].

ويختص كذلك بنوع محدد من الجرائم يتمثل في الجرائم التي سبق التفصيل فيها الجرائم الواردة في نص المادة 211 مكرر 24 من الأمر 21-11، والجرائم المتصلة بتكنولوجيات الإعلام والإتصال الأكثر تعقيدا والجرائم المرتبطة بها.

حيث لم يقتصر الاختصاص النوعي للقطب بالمتابعة والتحقيق والحكم في هذه الجرائم أي الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المتصلة بها في صورتها البسيطة، بل حتى تلك الأكثر تعقيدًا والجرائم المرتبطة بها، والجرائم الأكثر تعقيدا يُقصد بها الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب إتساع الرقعة الجغرافية لمكان إرتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين، ولتطلبها إستعمال وسائل وأساليب تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي[3].

[1] بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوالضياف، المسيلة، الجزائر، المجلد 07، العدد 01، جوان 2022، ص 1684.

[2] أنظر المادة 211 مكرر 22 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[3] أنظر المادة 211 مكرر 25، من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

ج _ الإختصاص المشترك للقطب الجزائي السيبراني:

_ إختصاص مشترك بين القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال والأقطاب الجزائية ذات الإختصاص الموسع:

نصت على هذا الإختصاص المادة 211 مكرر27 من الأمر رقم 21- 11 حيث أنه يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37 و40 و329 من قانون الإجراءات الجزائية الجزائري بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها[1].

وبالرجوع إلى المادة 37 من ق.إ.ج.ج في فقرتها الثانية[2]، والمادة 40 في فقرتها الثانية[3]، والمادة 329 في فقرتها الأخيرة[1] يتضح لنا وجود إختصاص مشترك بين القطب المستحدث والأقطاب الجزائية ذات الإختصاص الموسع في هذه الجرائم وهذا ما نصت عليه المادة 211 مكرر 27 من الأمر 21- 11.

[1] أنظر المادة 211 مكرر 27 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[2] تنص الفقرة 2 من المادة 37 من القانون رقم 14-04 المعدل والمتمم لقانون الإجراءات الجزائية " أنه يجوز تمديد الإختصاص المحلي لوكيل الجمهورية إلى دائرة إختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

[3] تنص الفقرة 2 من المادة 40 من القانون رقم 14-04 المعدل والمتمم لقانون الإجراءات الجزائية " يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة إختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

ثانيا: طرق إتصال القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بالقضايا

1_ إذا كان القطب الجزائي المستحدث يتمتع بإختصاص حصري:

يختص القطب بالجرائم المنصوص عليها بموجب المادتين 211 مكرر 24[2] و 211 مكرر 25[3] إذا كانت تشكل جنحا وفقا للفقرة 2 من المادة 211 مكرر 22[4].

ونصت المادة 211 مكرر 26 أنه تطبق على الإختصاص الحصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال الإجراءات المنصوص عليها في المواد من المادة 211 مكرر 19 إلى المادة 211 مكرر 21 من قانون الإجراءات الجزائية الجزائري.

حيث يتم إرسال التقارير الإخبارية وإجراءات التحقيق مباشرة من قبل مصالح الضبطية القضائية إلى وكيل الجمهورية بمحكمة مقر مجلس قضاء الجزائر، ويتلقى ضباط الشرطة القضائية حينئذ التعليمات منه مباشرة وفي حالة فتح تحقيق قضائي يتلقون الإنابات القضائية مباشرة من قاضي التحقيق المخطر بالملف[5].

---

[1] تنص الفقرة الأخيرة من المادة 329 ق.إ.ج.ج على أنه " يجوز تمديد الإختصاص المحلي للمحكمة إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف"

[2] أنظر المادة 211 مكرر 24 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[3] أنظر المادة 211 مكرر 25 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[4] أنظر المادة 211 مكرر 25 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[5] أنظر المادة 211 مكرر 19 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

إذا تبين لوكيل الجمهورية أن الوقائع المبلغة له لا تدخل ضمن إختصاصه، فإنه يصدر أمرا بعدم الإختصاص، فإنه يصدر مقررا بالتخلي لصالح وكيل الجمهورية المختص إقليميا[1].

إذا تبين لقاضي التحقيق أن الوقائع المخطر بها لا تدخل ضمن إختصاصه، يصدر أمر بعدم الإختصاص، إما تلقائيا بعد أخذ رأي وكيل الجمهورية وإما بناء على إلتماسات هذا الأخير. ثم يحول ملف الإجراءات بسعي من وكيل الجمهورية إلى النيابة العامة المختصة إقليميا متى أصبح أمر قاضي التحقيق نهائيا.

تبقى الأوامر بالقبض أو الإيداع الصادرة عن قاضي التحقيق سارية المفعول، تجدد إجراءات المتابعة والتحقيق وكذا الإجراءات الشكلية المتخذة قبل صدور الأمر بعدم الإختصاص[2].

2_ إذا كان القطب الجزائي المستحدث له إختصاص مشترك:

أ_ مع الأقطاب الجزائية الموسعة:

يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وكذا قاضي التحقيق ورئيس هذا القطب إختصاصا مشتركا مع الإختصاص الناتج عن تطبيق المواد 37 و40 و329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والإتصال والجرائم المرتبطة بها، ويتم تطبيق نفس الإجراءات المنصوص عليها في المواد من 211 مكرر 4 إلى 211 مكرر 15 من قانون الإجراءات الجزائية الجزائري المتبعة أمام القطب الجزائي الاقتصادي والمالي، كذلك أمام القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[3].

[1] أنظر المادة 211 مكرر 20 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 211 مكرر 21 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[3] أنظر المادة 211 مكرر 28 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

حيث يمارس وكيل الجمهورية للقطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مختلف صلاحياته تحت السلطة السلمية للنائب العام لدى مجلس قضاء الجزائر ويمارس صلاحيات النيابة العامة في القضايا التي تدخل ضمن اختصاصه[1].

ويخضع قاضي التحقيق ورئيس القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إداريا لسلطة رئيس مجلس قضاء الجزائر[2].

ثم يقوم وكلاء الجمهورية لدى الجهات القضائية المختصة إقليميا وفقا لأحكام المادة 37 من هذا القانون، بارسال بكل الطرق وعلى الفور، نسخا من التقارير الإخبارية وإجراءات التحقيق التي أنجزتها الشرطة القضائية في إطار هذه الجرائم إلى وكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[3]، ثم يطالب هذا الأخير بالملف الإجرائي بعد أن يأخذ رأي النائب العام لدى مجلس قضاء الجزائر، إذا رأى أن الجريمة تدخل ضمن إختصاصه[4].

ويجوز لوكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، المطالبة بملف الإجراءات أثناء القيام بالتحري والمتابعة والتحقيق القضائي[5].

وخلال مرحلتي التحقيق الأولي والمتابعة، وبعد تقديم التماسات وكيل الجمهورية لدى القطب ومطالبته بالملف الإجرائي، يصدر وكيل الجمهورية المختص اقليما مقررًا بالتخلي عن الملف لصالح وكيل الجمهورية لدى القطب[6].

[1] أنظر المادة 211 مكرر 4 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
[2] أنظر المادة 211 مكرر 5 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
[3] أنظر المادة 211 مكرر 6 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
[4] أنظر المادة 211 مكرر 7 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
[5] أنظر المادة 211 مكرر 8 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.
[6] أنظر المادة 211 مكرر 9 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

وإذا ما تم فتح تحقيق قضائي، يحيل وكيل الحمهورية على قاضي التحقيق المخطر بالملف، الالتماسات التي قدمها وكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال لغرض المطالبة بالملف، وعليه يصدر قاضي التحقيق أمرا بالتخلي لفائدة قاضي تحقيق القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[1].

في حالة تمت المطالبة بملف الإجراءات في وقت واحد من طرف وكيل الجمهورية لدى القطب الجزائي المتخصص، ومن طرف وكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، فإن الاختصاص يؤول إلى هذا الأخير.

أضف إلى ذلك في مرحلة التحري أو المتابعة أو التحقيق القضائي إذا تواجد الملف على مستوى الأقطاب الجزائية ذات الاختصاص الإقليمي الموسع، فإن هذه الجهة الأخيرة تتخلي عن الملف، في حالة ما إذا تم طلبه من قِبل وكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، وفقا لما هو منصوص عليها في المادتين 211 مكرر 9 و211 مكرر 10[2].

ثم يتم إرسال الملف مرفوقا بجميع الأوراق والأدلة من وكيل الجمهورية المختص إلى وكيل الجمهورية لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال[3].

جميع الأوامر بالقبض وأوامر الوضع رهن الحبس المؤقت التي أصدرها قاضي تحقيق الجهة القضائية الموسعة تبقى منتجة لآثارها إلى أن يصدر أمر مخالف عن قاضي التحقيق

[1] أنظر المادة 211 مكرر 10 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 211 مكرر 11 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[3] أنظر المادة 211 مكرر 12 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

بالقطب القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال أمر مخالف، ويصبح هذا الأخير ضامن لصحة إجراءات الحبس المؤقت وشرعيتها[1].

وبمجرد التخلي عن ملف الإجراءات من الجهات القضائية ذات الاختصاص الموسع، تحول سلطات إدارة ومراقبة أعمال الضبطية القضائية بشأن الإجراءات التي تمت أو التي قيد التنفيذ أو التي سيتم إتخاذها، إلى وكيل الجمهورية وقاضي التحقيق لدى القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ويتلقون منهما التعليمات والانابات القضائية[2].

ب_ مع القطب الاقتصادي والمالي:

عندما يكون للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال إختصاص متزامن مع القطب الإقتصادي والمالي في هذه الحالة فإن الإختصاص يؤول وجوبا إلى القطب الإقتصادي والمالي[3]، وبالتالي يتم التخلي عن ملف القضية في أي مرحلة كان في هذه الحالة لصالح القطب الإقتصادي والمالي وجوبا.

ج_ مع إختصاص محكمة مقر مجلس قضاء الجزائر:

في الحالة التي يتزامن فيها إختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال مع إختصاص محكمة مقر مجلس قضاء الجزائر فإنه يمارس وكيل الجمهورية وقاضي التحقيق بمحكمة مقر مجلس قضاء الجزائر صلاحيتهما في كامل الإقليم الوطني[4]، وعليه فإنه إذا كان ملف القضية عند وكيل

[1] أنظر المادة 211 مكرر13 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[2] أنظر المادة 211 مكرر14 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

[3] أنظر المادة 211 مكرر28 من الأمر رقم 21-11 المتمم لقانون الإجراءات الجزائية الجزائري.

[4] أنظر المادة 211 مكرر16 من الأمر رقم 20- 04 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري.

الجمهورية لدى القطب الجزائي المستحدث في مرحلة المتابعة فإنه يتخلى عليه لصالح وكيل الجمهورية لمحكمة مقر المجلس، وكذلك الأمر إذا كان الملف عند لدى قاضي التحقيق للقطب الجزائي المستحدث فإنه يتخلى عليه لصالح قاضي التحقيق لدى محكمة مقر المجلس.

خلاصة الباب الثاني:

أصبحت التهديدات السيبرانية هاجس يهدد أمن الأشخاص وأموالهم وحياتهم الخاصة، فتعددت وتنوعت هذه التهديدات، وأخطرها تلك التي تتخذ شكل جرائم متعلقة بأنظمة المعالجة الآلية للمعطيات بمختلف أشكالها، والتي قد تبرز في شكل الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تتخذ شكل الجرائم الواقعة على معطيات أنظمة المعالجة الآلية التي تمثل العناصر المنطقية لهذا الأخير، ولا يهم هنا إن كانت معطيات عامة، أم من فئات خاصة منها كالمعطيات الشخصية، فهذه الجرائم تعتبر من الجرائم المعلوماتية البحتة –كما يُطلق عليها– والتي يكون محلها نظام المعالجة الآلية للمعطيات، وهناك جرائم يكون هذا الآخير أي نظام المعالجة الآلية للمعطيات مسهلا لإرتكابها أو وسيلة لارتكابها، وتتمثل في جل الجرائم التقليدية المعروفة التي تستخدم في ارتكابها هذه الأنظمة، إضافة إلى جرائم مواقع التواصل الاجتماعي التي استفحلت في الآونة الأخيرة، حيث تطرقنا إلى أهم نموذجين مستحدثين منها ومتمثلين في جرائم التمييز والكراهية عبر مواقع التواصل الإجتماعي، وجريمة نشر الأخبار الكاذبة.

وبالموزاة مع ما هو موجود على المستوى الدولي، تم إنتهاج سياسة جنائية وطنية لمكافحة هذه الجرائم، انعكست على التجريم والعقاب في الشق الموضوعي، وعلى الآليات الإجرائية في الشق الإجرائي فتم تحديث قانون العقوبات وتطويره، وتم النص على قانون مستحدث لحماية المعطيات الشخصية المعالجة بواسطة هذه الانظمة، وفي شقها الإجرائي جاءت بتدابير إجرائية تشمل الوقاية والمنع من إرتكاب هذه الجرائم، وتم إستحداث قواعد قانونية إجرائية لمكافحتها في مختلف المراحل من المتابعة إلى غاية المحاكمة تتماشى ومتطلبات السياسة الجنائية المعاصرة.

خاتمة

خاتمة:

وفي ختام هذه الدراسة تتضح لنا "**السياسة الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات**" على المستوى الدولي والوطني، ويبرز دور منظمة الأمم المتحدة الذي يتجسد من خلال جهودها الدولية المتمثلة في المؤتمرات الدولية والقرارات الدولية، في توجيه هذه السياسة الجنائية على المستوى العالمي، رغم غياب اتفاقية عالمية بهذا الشأن، وبرز لنا كذلك دور المنظمات الإقليمية على المستوى الأوروبي والعربي والإفريقي في توجيه هذه السياسة الجنائية على المستوى الاقليمي.

ولتفعيل السياسة الجنائية الموضوعية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، تطلبت خصوصية الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وعبورها للحدود الوطنية، ضرورة تنسيق التعاون الجنائي الدولي في المجال الإجرائي.

والمشرع الوطني سعى لتحقيق سياسة جنائية شاملة ومتكاملة ومتناسقة لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، حيث يتجلى لنا من خلال هذه الدراسة أن المشرع الجزائري خطى خطوة كبيرة بشأن تطوير تشريعاته الوطنية المطبقة على الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بما يتماشى والتزاماته الدولية هذا من جهة، ومع متطلبات السياسة الجنائية المعاصرة من جهة أخرى، وهذا لغرض التصدي لهذا النوع من الإجرام المستحدث الذي يتطلب خصوصية في التجريم وفي إجراءات المتابعة والتحقيق والمحاكمة، لغرض معاقبة المجرمين المعلوماتيين وتجسيد مبدأ عدم الإفلات من العقاب، والموازنة بين حق المجتمع وحقوق هؤلاء المجرمين.

ومن أهم النتائج والاقتراحات التي توصلنا إليها في هذه الدراسة:

أولا: النتائج

01_ غياب إتفاقية دولية عالمية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وإتفاقية عالمية كذلك لمكافحة الجرائم المتعلقة بالمعطيات الشخصية.

02_ تنوع وكثرة التشريعات والاتفاقيات الدولية على المستويين الإقليمي، راجع للرغبة الدولية المشتركة في تطوير سياستها الجنائية وتماشيها مع تطور هذه الظاهرة الإجرامية المرنة، هذا إيجابي من جهة، وسلبي من جهة أخرى بسبب كثرة، وتباين هذه التشريعات وتداخلها.

03_غياب تشريع على المستوى الإقليمي العربي خاص بمكافحة الجرائم المتعلقة بالمعطيات الشخصية.

04_ تبني الجزائر القانون العربي النموذجي لمكافحة جرائم تقنية المعلوماتية كونه من أكثر الاتفاقيات الملائمة لهذه الجريمة، ورغم عدم مصادقتها على اتفاقية بودابست التي تعتبر من أهم الاتفاقيات لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، إلا أن المشرع الجزائري انتهج النهج الذي سلكته هذه الأخيرة في شقها الموضوعي لاسيما في التجريم و البناء القانوني لهذه الجرائم.

05_ وجود العديد من المشاكل بخصوص مبدأ الإقليمية والمتعلقة بتحديد موقع الجريمة.

06_ رغم تحديد المشرع الجزائري لغالبية تعاريف المصطلحات في قوانينه الموضوعية والإجرائية المرتبطة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات إلا أنه استخدم تعريفات فضفاضة وغير دقيقة، لإضفاء المرونة على هذه النصوص لكي لا يتجاوزها الزمن، حيث اعتماد المشرع الجزائري على أسلوب " التجريم المفتوح" في هذه النصوص، وهذا يتعارض مع مبدأ الشرعية الذي يستوجب التجريم المحدد والدقيق.

07_ الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات منها ما يكون الاعتداء فيها واقع على النظام في حد ذاته ومنها ما يستهدف الاعتداء على معطياته ومنها ما يكون الاعتداء بواسطة أنظمة المعالجة الآلية للمعطيات واستخدامها كوسيلة.

08_ نجد تكامل بين قانون العقوبات الجزائري والقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقانون الإجراءات الجزائية الجزائري والقانون رقم 09- 04 المتعلق بتكنولوجيات الإعلام والاتصال وتماشوا مع

السياسة الجنائية المعاصرة، حيث الأول أقر حماية جنائية موضوعية لأنظمة المعالجة الآلية للمعطيات من خلال التجريم بأنواعه فأورد فيه جرائم الضرر، وجرائم الخطر التي يكون فيها التجريم وقائي، حيث يكون قبل إرتكاب الجريمة والمساس بنظام المعالجة الآلية للمعطيات، وذلك بمجرد الدخول والبقاء، في نظام المعالجة الآلية للمعطيات حمايةً للحقوق من المساس حيث تعتبر هذين الجريمتين من جرائم الخطر، وكذلك أورد العقوبات المقررة للمجرمين المعلوماتيين، وأورد قانون الإجراءات جزائية الجزائري الأحكام العامة الإجرائية المطبقة على هذه الجرائم، وأورد القانون 09-04 إجراءات وتدابير وقائية كذلك يمكن إتخاذها قبل إرتكاب الجريمة وذلك بغرض الوقاية منها كإجراء "مراقبة الإتصالات الإلكترونية الوقائي"، "التفتيش والحجز الوقائي" وقيدها بشروط وهذا ضمانا لإحترام الحق في الحياة الخاصة.

أما القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الذي جرم هو الأخر الأفعال التي تشكل إعتداء على المعطيات الشخصية وأَفْرَدَ لكل جريمة العقوبات الخاصة بها، وأورد أحكاما إجرائية.

وكلا من القانون 18-07 والقانون 09-04 نصا على سلطات إدارية مستقلة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال.

09_ تم استحداث إجراءات تتماشى وخصوصية الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات محلها البيئة السيبرانية تتمثل في تفتيش المنظومة المعلوماتية ككل أو جزء منها.

10_ تم استحداث جهات قضائية موسعة الاختصاص لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، واستحداث جهات أخرى يمتد اختصاص لكامل التراب الوطني.

11_ إهمال ضحايا هذه الجرائم وهذا يتنافى مع مقاصد السياسة الجنائية المعاصرة التي تهتم بالضحية والمجرم على حد سواء.

12 _ غياب تام للاجتهادات القضائية في مجال الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، وكما نعلم أنه من صفات القاضي بصفة عامة والقاضي الجزائي بصفة خاصة البحث والاجتهاد ووجود حل للمشاكل المتعلقة بهذا النوع من الجرائم.

ثانيا: الاقتراحات

في ضوء ما أبرزته لنا دراسة "السياسة الجنائية لمكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات" ولسد النقص في السياسية الدولية والوطنية لمكافحتها، وتأكيدًا على ضرورة مكافحة هذا النوع من الجرائم، نقترح الاقتراحات التالية:

01_ الدعوة إلى توحيد الجهود الدولية وتنسيق التعاون الدولي من خلال تبني إتفاقية دولية عالمية وحيدة في مجال مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، لتساهم في تحديد الإطار التشريعي والمرجعي على المستوى العالمي من خلال وضع نموذج تجريمي واضح، بغرض مواءمة التشريعات الوطنية معه، ولتوحيد الجهود وتنسيق التعاون الدولي، مثلما هو معمول به في مجال مكافحة الجريمة المنظمة وذلك بهدف إختصار الوقت، وتسريع الإجراءات عند تفعيل آليات التعاون الدولي.

02_ ندعو إلى النص على مبدأ العالمية وتطبيقه صراحة بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

03_ يتعين تبيان المعايير التي يعتمدها القضاء الجزائري في تحديد موقع الجريمة المتعلقة بأنظمة المعالجة الآلية للمعطيات، بما يتوافق مع خصوصية هذه الجريمة.

04_ تحديث القواعد والأحكام القانونية للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تماشيا مع تطورات هذه الجرائم المستمرة وتماشيا مع أساليب إرتكابها وخصوصية إجراءاتها.

05_ ضرورة تعديل القانون رقم 09-04 والنص على التسرب الإلكتروني كأسلوب تحري خاص في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

06_ إقرار مبدأ تخصص القاضي الجنائي، باعتباره من الضرورات التي تمليها السياسة الجنائية المعاصرة، ويتجسد هذا من خلال تكوين القضاة في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تكوينًا متخصص في هذا الشأن منذ الدراسة في المدرسة العليا للقضاء إلى غاية تخرجهم كقضاة، ويتواصل تحديث وتحيين تكوينهم وتدريبهم طيلة فترة مسارهم العملي، لأن هذه الجرائم تتطور أساليب ارتكابها يوميا.

07_ تشريع قانون خاص بهذا النوع من الجرائم ويطلق عليه تسمية " قانون مكافحة الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات وإساءة استخدام تكنولوجيات الإعلام والاتصال والوقاية منها " يشتمل على القواعد الموضوعية والإجرائية معًا، والوقائية، وذلك من خلال نقل إليه المواد من 394 مكرر إلى 394 مكرر8 من قانون العقوبات، والنصوص القانونية الواردة في القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، لأن هذا الأخير يشتمل فقط على الجانب الإجرائي دون الموضوعي مثل ما هو معمول به في مختلف القوانين الخاصة كالقانون 06-01 المتعلق بالوقاية من الفساد ومكافحته.

وبالتالي وضع نموذج تجريمي واضح للجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، ويقابله الشق الإجرائي، وهذا بغرض تجنب التضخم التشريعي إذا ما حصل تطور في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات والجرائم الناجمة عن اساءة استخدام تكنولوجيات الاعلام والاتصال مستقبلا، وأدى هذا التطور إلى تشريع قوانين أخرى لمكافحة هذه الجرائم المستجدة وتحدياتها المستقبلية، مما يجعل التشريعات الخاصة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات تتزايد، وتتشعب، وبالتالي فبسن تشريع خاص بهذه الجرائم إذا ما حصل تطور يكون التعديل فيه هو بحد ذاته.

08_ بالنسبة للقواعد الموضوعية يجب كذلك نص المشرع على مختلف الجرائم التقليدية في صورتها الحديثة لأنه يوجد فراغ تشريعي عندما ترتكب جريمة تقليدية بواسطة نظام المعالجة الآلية للمعطيات أو يسهل هذا الأخير ارتكابها، يتم تطبيق القواعد القانونية التقليدية، فعلى

الأقل يتم تشديد عقوباتها حتى لا تخضع للأحكام العقابية التقليدية المنصوص عليها في قانون العقوبات .

09_ ضرورة تجريم الاعتداء على البريد الالكتروني ومواقع التواصل الاجتماعي والحسابات الخاصة بموجب نص قانوني واضح وصريح تماشيا مع مبدأ الشرعية.

10_ النص على عقوبات تكميلية إضافة إلى تلك المنصوص عليها في المادة 9 من ق.ع.ج تتمثل في حرمان المحكوم عليه بسبب ارتكابه جريمة من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات من استخدام أي شبكة إلكترونية أو منظومة معلوماتية أو وسيلة من وسائل تكنولوجيات الاعلام والاتصال لمدة محددة ابتداء من يوم انقضاء العقوبة الأصلية مثلما تم النص عليه في القسم الأول مكرر الموسوم ب: الإهانة والتعدي على المؤسسات الصحية ومستخدميها.

11_ إنشاء محاكم متخصصة بالجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات بمختلف أشكالها، ولا تكون تقتصر إلا على الخطيرة منها مثلما هو معمول به حاليا أمام الجهات القضائية الجزائية ذات الاختصاص الموسع، والقطب الجزائي المتخصص بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإنما تشمل هذا النوع من الجرائم بمختلف أشكالها وباختلاف درجة خطورتها، واعتماد هذه المحاكم على إجراءات التقاضي الإلكتروني خاصة في مرحلتي المتابعة والتحقيق من خلال استخدام إجراء المعاينة الرقمية، وإجراءات التفتيش وحجز معطيات المنظومة المعلوماتية، إضافة إلى التسرب الإلكتروني، والخبرة الرقمية، واستخدام أدلة الإثبات الرقمية مثلما هو معمول به في غالبية الدول.

12_ يتعين إنشاء جهة قضائية استئنافية متخصصة توازي القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الأعمال والاتصال حتى لا يكون استئناف الأحكام الصادرة عن هذا القطب المستحدث أمام مجلس قضاء الجزائر العاصمة، وكذلك الأمر بالنسبة لاستئناف أوامر قاضي التحقيق الذي يكون أمام غرفة إتهام مجلس القضاء الجزائر العاصمة، لأنه كما نعلم أن عند استئناف الأحكام يتم النظر في القضية برمتها وبالتالي من

المستحسن أن يكون هناك جهة استئناف متخصصة في هذا النوع من الجرائم التي تستوجب خصوصية في إجراءات المتابعة والتحقيق.

13_ يتعين إستحداث قاعدة معطيات وطنية تخص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، بغرض تسهيل تبادل الملفات بين القطب الجزائي الوطني والجهات القضائية ذات الاختصاص الموسع والمحاكم العادية.

14_ تكوين العناصر البشرية (الضبطية القضائية)، تكوينا متخصصا في الوقاية القبلية والوقاية البعدية من هذا النوع من الجرائم حتى لا تتفاقم أكثر.

15 _ تكوين القضاة تكوين قانونيا وفنيا وتقنيا يتناسب مع هذا النوع من الجرائم، وتأهيلهم وتدريبهم تدريب قانوني وتكوين علمي يشمل أهم العلوم المتصلة بهذه الجرائم والتي تُسهل الكشف عنها، كعلوم كشف الجريمة بالوسائل الحديثة، وعلم الطب الشرعي الرقمي الذي يعتبر من أحدث العلوم في مجال الطب الشرعي، فهو يكشف على المعطيات الرقمية والبيانات، ويفسرها لأجل الحفاظ على الدليل الرقمي في شكله الأصلي.

إضافة إلى علم العلوم الجنائية الرقمية الذي يعتبر من فروع العلوم الجنائية الذي يهتم بالاسترداد والبحث في أنظمة المعالجة الآلية للمعطيات التي تحتوي بيانات ومعطيات رقمية، والتحقيق الجنائي الرقمي واستخراج الدليل الرقمي، ويستخدم كذلك الطب الشرعي الرقمي في التحقيق، وتحديد الأدلة الرقمية.

16_ تشجيع التبليغ الإلكتروني عن هذا النوع من الجرائم من خلال إستحداث منصة رقمية خاصة بالتبليغ عنها بمختلف أنواعها تبليغ آنيا وقت اكتشافها حتى لا تستفحل أكثر بسبب التلاعب بالدليل الرقمي من خلال حذفه أو التغيير فيه لأنه سريع الحذف والتغيير والتشفير.

17_ إنشاء آلية إخطار وقائية بالنسبة للأشخاص المعنوية العامة خاصةً لكثرت الاعتداءات عليها، وكذلك بالنسبة للأشخاص المعنوية الخاصة، للتبليغ عن التهديدات والمساس

بمتطلبات السلامة والابلاغ لحظة إدراك التهديد السيبراني وقبل المساس بنظام المعالجة الآلية للمعطيات.

18_ استحداث تخصص جديد في تكوين طلبة القانون في الماستر، يتمثل في تدريس القانون الجنائي الرقمي كفرع من فروع القانون الجنائي باعتباره قانون مستحدث بالجامعات لطلبة القانون الذين يعتبرون هم رجال القانون في المستقبل يشكلون (القضاة، الضبطية القضائية، المحامين) يشتمل على عدة مقاييس تتمثل في: القانون المعلوماتي الموضوعي (التجريم الإستباقي للوقاية من الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، العقاب في الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، القانون المعلوماتي الإجرائي (التفتيش الرقمي، التحقيق الرقمي، حجز المعطيات الرقمية، أدلة الإثبات الرقمية (إستخراج الأدلة الرقمية، طرق التعامل مع الأدلة الرقمية)، المحاكم الرقمية التي تتناسب مع هذه الجرائم. لأنه أصبح يُتنبؤ حاليا بإختفاء شبه تام للجرائم التقليدية في المستقبل والتوجه نحو الجرائم المتعلقة بأنظمة المعالجة الآلية واستخدام الذكاء الاصطناعي في ارتكابها.

19_ نشر ثقافة الأمن السيبراني، وزيادة الوعي بخصوص الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات.

قائمة المصادر

والمراجع

قائمة المصادر والمراجع:

المصادر والمراجع باللغة العربية:

أولا: المصادر باللغة العربية

1_ المصادر الخارجية:

أ_ الاتفاقيات الدولية والمواثيق:

1_ ميثاق الأمم المتحدة الصادر بتاريخ 26 جوان 1945، بسان فرانسيسكو بالولايات المتحدة الامريكية، (تاريخ النفاذ: 24 أكتوبر 1945).

2_ الاعلان العالمي لحقوق الإنسان الذي اعتمد بموجب قرار الجمعية العامة للأمم المتحدة رقم 217 ألف، الدورة 3، المؤرخ في 10 ديسمبر 1948.

3_ الإتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية، الصادرة عن المجلس الأوربي، الموقعة، الموقعة في روما بتاريخ 04 نوفمبر 1950.

4_ القانون الأساسي للمنظمة الدولية للشرطة الجنائية_ الإنتربول، الدورة 25 للجمعية العامة المنعقدة في فيينا بتاريخ 13 يونيو 1956.

5_ العهد الدولي للحقوق المدنية والسياسية، الذي اعتمد بموجب قرار الجمعية العامة للأمم المتحدة رقم 2200 ألف، الدورة21، المؤرخ في 16 ديسمبر 1966.

6_ إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة بموجي قرار رقم 25/55 بتاريخ 15 نوفمبر سنة 2000، المصادق عليها بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فيفري 2002، ج.ر.ج.ج، عدد 09، صادر بتاريخ 10 فيفري 2002.

7_ الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، القاهرة، 21 ديسمبر 2010، المصادق عليها من طرف الجزائر

بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في 13 ذي القعدة عام 1435 الموافق ل 8 سبتمبر 2014، ج. ر.ج.ج العدد57،المؤرخة في 28 سبتمبر 2014.

ب_ البروتوكولات الإضافية:

1_ البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الالكترونية بشأن تعزيز التعاون والكشف عن الأدلة الالكترونية الصادر عن مجلس أوربا سنة 2021.

ج_ التقارير التفسيرية للاتفاقيات:

1_ التقرير التفسيري لإتفاقية الجريمة الإلكترونية، مجلس أوربا، سلسلة المعاهدات الأوروبية رقم 185، بودابست، المجر، 23 نوفمبر 2001.

2_ التقرير التفسيري للبروتوكول الإضافي لإتفاقية الجريمة الالكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر، سلسلة المعاهدات الأوربية رقم 169، مجلس أوربا، الصادر بستراسبورغ بتاريخ 28 يناير/ كانون الثاني 2003. متوفر على الرابط التالي:

https://rm.coe.int/explanatory-report-additional-protocol-on-xenophobia-and-racism-in-ara/1680739176

د_ قرارات منظمة الأمم المتحدة:

_قرارات الجمعية العامة:

1_ مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة45/95 المؤرخ في 14 كانون الأول/ديسمبر 1990.

2_ قرار الجمعية العامة رقم 49/53، التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي ، المؤرخ في 1 ديسمبر 1999.

3_ قرار الجمعية العامة رقم 70/53، التطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 63، من جدول أعمال الدورة 53، الصادر المؤرخ في 4 كانون الأول/ ديسمبر 1998.

4_ القرار رقم 28/55 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 68 من جدول أعمال الدورة 55، المؤرخ في 20 نوفمبر 2000.

5_ قرار الجمعية العامة رقم 63/55 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 105 من جدول أعمال الدورة 55، المؤرخ في 4 كانون الأول/ ديسمبر 2000.

6_ قرار الجمعية العامة رقم 19/56 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 69 من جدول أعمال الدورة 56، المؤرخ في 29 نوفمبر 2001.

7_ قرار الجمعية العامة رقم 121/56 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 110 من جدول أعمال الدورة 56، المؤرخ في 19 كانون الأول/ ديسمبر 2001.

8_ قرار الجمعية العامة رقم 239/57، إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي، البند 84 (ج) من جدول الأعمال، الدورة 57، الصادر بتاريخ 31 / 01/ 2003.

9_ قرار الجمعية العامة رقم 58/ 32 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 68 من جدول أعمال الدورة 58، المؤرخ في 8 ديسمبر 2003.

10_ قرار الجمعية العامة رقم 61/59 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 60 من جدول أعمال، الدورة 59، المؤرخ في 3 كانون الأول/ ديسمبر 2004.

11_ قرار الجمعية العامة رقم 45/60 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 86 من جدول أعمال الدورة 60، المؤرخ في 8 كانون الأول/ ديسمبر 2005.

12_ قرار الجمعية العامة رقم 17/62 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 62، المؤرخ في 5 كانون الأول/ ديسمبر 2007.

13_ قرار الجمعية العامة رقم 37/63 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 85 من جدول أعمال الدورة 63، المؤرخ في 2 كانون الأول/ ديسمبر 2008.

14_ قرار الجمعية العامة رقم 25/64 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 91 من جدول أعمال الدورة 64، المؤرخ في 2 كانون الأول/ ديسمبر 2009.

15_ قرار الجمعية العامة رقم 41/65 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 85 من جدول أعمال الدورة 65، المؤرخ في 8 كانون الأول/ ديسمبر 2010.

16_ قرار الجمعية العامة رقم 24/66 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 66، المؤرخ في 2 كانون الأول/ ديسمبر 2011.

17_ قرار الجمعية العامة رقم 181/66 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 107 من جدول أعمال الدورة 66، المؤرخ في 19 كانون الأول/ ديسمبر 2011.

18_ قرار الجمعية العامة رقم27/67 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 89 من جدول أعمال الدورة 67، المؤرخ في 3 كانون الأول/ ديسمبر 2012.

19_ قرار الجمعية العامة رقم 167/68 المعنون ب الحق في الخصوصية في العصر الرقمي، البند 69 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الثاني/ ديسمبر 2013.

20_ قرار الجمعية العامة رقم 193/68 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 108 من جدول أعمال الدورة 68، المؤرخ في 18 كانون الأول/ ديسمبر 2013.

21_ قرار الجمعية العامة رقم243/68 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 94 من جدول أعمال الدورة 68، المؤرخ في 27 كانون الأول/ ديسمبر 2013.

22_ قرار الجمعية العامة رقم 28/69 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 91 من جدول أعمال الدورة 69، المؤرخ في 2 كانون الأول/ ديسمبر 2014.

23_ قرار الجمعية العامة رقم 166/69 المعنون ب الحق في الخصوصية في العصر الرقمي، البند 68 (ب) من جدول أعمال الدورة 68، الصادر بتاريخ 18 كانون الثاني/ ديسمبر 2014.

24_ قرار الجمعية العامة رقم 237/70 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 92 من جدول أعمال الدورة 70، المؤرخ في 23 كانون الأول/ ديسمبر 2015.

25_ قرار الجمعية العامة رقم 27/71 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 93 من جدول أعمال الدورة 71، المؤرخ في 2 كانون الأول/ ديسمبر 2016.

26_ قرار الجمعية العامة رقم 196/72 المعنون بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولاسيما قدراته في مجال التعاون التقني، البند 107 من جدول أعمال الدورة 72، المؤرخ في 19 كانون الأول/ ديسمبر 2017.

27_ قرار الجمعية العامة رقم 27/73 المعنون بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي، البند 96 من جدول أعمال الدورة 73، المؤرخ في 5 كانون الأول/ ديسمبر 2018.

28_ قرار الجمعية العامة رقم 187/73 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 109 من جدول أعمال الدورة 73، المؤرخ في 17 كانون الأول/ ديسمبر 2018.

29_ قرار الجمعية العامة رقم 282/75 المعنون بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، البند 112 من جدول أعمال الدورة 75، المؤرخ في 26 أيار/ مايو 2021.

هـ_ القرارات التي اعتمدتها مؤتمرات الأمم المتحدة:

1_ القرار رقم 1 الذي اعتمده مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، إعلان سلفادور بشأن الاستراتيجيات الشاملة لمواجهة التحديات العالمية: نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير،السلفادور، البرازيل، 12-19 نيسان/أبريل 2010، A/conf.213/18. متوفر على الرابط التالي:
https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_A.pdf

2_ المصادر الداخلية:

أ_ الدساتير:

1_ مرسوم رئاسي رقم 20_442 مؤرخ في 15 جمادى الأولى عام 1442 الموافق ل 30 ديسمبر سنة 2020، يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020، ج.ر.ج.ج، العدد 82، المؤرخة في 30 ديسمبر سنة 2020.

ب_ القوانين العضوية:

1_ القانون العضوي رقم 12- 05 مؤرخ في 18 صفر عام 1433 الموافق 12 يناير سنة 2012، المتعلق بالإعلام، ج.ر.ج.ج العدد02، المؤرخة في 21 صفر عام 1433هـ الموافق 25 يناير سنة 2012.

ج_ القوانين العادية:

1_ القانون رقم 04-14 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، المعدل والمتمم للأمر رقم 66-155، المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج العدد 71، ج.ر.ج.ج المؤرخة في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

2_ القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج، العدد 71، المؤرخة في 27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004.

3_ القانون رقم 06- 22 المؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر سنة 2006، المعدل والمتمم لقانون الإجراءات الجزائية الجزائري، ج.ر.ج.ج، العدد84، المؤرخة في 4 ذو الحجة عام 1427 الموافق 4 ديسمبر 2006.

4_ القانون رقم 06- 23 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 ، يعدل ويتمم الأمر 66- 156 المتضمن قانون العقوبات، ج. ر.ج.ج، العدد84، المؤرخة في 4 ذي الحجة عام 1427 هـ، الموافق 24 ديسمبر سنة 2006.

5- القانون رقم 09- 04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47، المؤرخة في 25 شعبان عام 1430، الموافق ل16 غشت سنة 2009.

6_ القانون رقم 14- 04 المؤرخ في 24 ربيع الثاني عام 1435 الموافق 24 فبراير سنة 2014، المتعلق بالنشاط السمعي البصري، ج. ر.ج.ج العدد 16 الصادرة في 21 جمادى الأولى عام 1435 هـ الموافق 23 مارس سنة 2014.

7_ الأمر 15-02 المؤرخ في 07 شوال عام 1436 الموافق 23 يوليو سنة 2015، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج العدد 40، االمؤرخة في 7 شوال عام 1436 الموافق 23 يوليو سنة 2015.

8_ القانون رقم 15-04 المؤرخ في 11 ربيع الثاني عام 1436 الموافق أول فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، ج.ر.ج.ج، العدد 06، الصادرة في 20 ربيع الثاني عام 1436 هـ الموافق 10 فبراير سنة 2015.

9_ القانون رقم 15- 12 المؤرخ في 28 رمضان عام 1436 الموافق 15 يوليو سنة 2015 المتعلق بحماية الطفل، ج.ر.ج.ج، العدد 39، الصادرة بتاريخ 3 شوال عام 1436 هـ الموافق 19 يوليو سنة 2015.

10_ القانون رقم 16- 02 المؤرخ في 19 يونيو 2016 المعدل والمتمم لقانون العقوبات، مؤرخ في 14 رمضان عام 1437 الموافق 19 يونيو 2016، ج.ر.ج.ج، العدد37، مؤرخة في17 رمضان عام 1437 الموافق 22 يونيو 2016.

11_ القانون رقم 17-07 مؤرخ في 28 جمادى الثانية عام 1438 الموافق 27 مارس سنة 2017، يعدل ويتمم الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 20، المؤرخة في أول رجب عام 1438 هـ الموافق 29 مارس سنة 2017م.

12_ القانون رقم 18-04 المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو 2018، يحدد القواعد المتعلقة بالبريد والإتصالات الإلكترونية، ج.ر.ج.ج ، العدد 27، المؤرخة في 27 شعبان عام 1439 الموافق ل 13 مايو سنة 2018.

13_ القانون 18-07 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ج.ج، العدد 34، المؤرخة في 25 رمضان عام 1439 الموافق ل 10 يونيو سنة 2018.

14_ القانون رقم 19- 10 المؤرخ في 14 ربيع الثاني عام 1444 الموافق 11 ديسمبر سنة 2019، يعدل الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 78 المؤرخة في 21 ربيع الثاني عام 1441 هـ الموافق 18 ديسمبر سنة 2019.

15_ الأمر رقم 20-04 مؤرخ في 11 محرم عام 1442 الموافق 30 غشت سنة 2020، يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 51 مؤرخة في 12محرم عام 1442، الموافق 31 غشت 2020.

16_ القانون رقم 20-05 المؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر.ج.ج، العدد 25، المؤرخة في 6 رمضان عام 1441هـ الموافق ل 29 أبريل سنة 2020.

17_ القانون رقم 20_06 المؤرخ في 5 رمضان عام 1441 الموافق 28 أفريل 2020 المعدل والمتمم لقانون للأمر رقم 66-156 المتضمن قانون العقوبات، ج.ر.ج.ج، العدد 25 المؤرخة في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020.

18_ الأمر رقم 21- 11 المؤرخ في 16 محرم عام 1443 الموافق 25 غشت سنة 2021، يتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج، العدد 65 المؤرخة في 17 محرم عام 1443 هـ الموافق 26 غشت سنة 2021.

د_القوانين التنظيمية:

_ المراسيم الرئاسية:

1_ المرسوم الرئاسي رقم 04- 183 مؤرخ في 8 جمادى الأولى عام 1425 الموافق 26 يونيو 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج العدد 41 مؤرخة في 9 جمادى الأولى عام 1425 الموافق 27 يونيو 2004.

2_ المرسوم الرئاسي رقم 15-261 مؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج.ر.ج.ج العدد53، المؤرخة في 24 ذو الحجة عام 1436هـ الموافق 8 أكتوبر سنة 2015.

3_ المرسوم الرئاسي رقم 20-05 المؤرخ في 24 جمادى الأولى عام 1441 الموافق 20 جانفي سنة 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج. ر.ج. ج، العدد04، المؤرخة في أولى جمادى الثانية عام 1442هـ الموافق 26 جانفي سنة 2020.

4_ المرسوم الرئاسي رقم 20- 183 مؤرخ في 21 ذي القعدة عام 1441 الموافق 13 يوليو سنة 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، ج.ر.ج.ج العدد 40 المؤرخة في 26 ذي القعدة عام 1441 هـ الموافق ل 18 يوليو سنة 2020.

5_ المرسوم التنفيذي رقم 20- 332 المؤرخ في 80 ربيع الثاني عام 1442 الموافق 22 نوفمبر 2020، الذي يحدد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، ج ر ج ج، العدد 70 الصادرة في 25 نوفمبر 2020.

6_ المرسوم الرئاسي رقم 21- 439 مؤرخ في 2 ربيع الثاني عام 1443 الموافق 7 نوفمبر سنة 2021، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات

الإعلام والاتصال ومكافحته، ج.ر.ج.ج العدد 86 المؤرخة في 6 ربيع الثاني عام 1443هـ الموافق ل 11 نوفمبر سنة 2021.

7_ المرسوم الرئاسي رقم 22-187 المؤرخ في 17 شوال عام 1443 الموافق 18 ماي سنة 2022، يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، ج.ر.ج.ج العدد 35، المؤرخة في 23 شوال 1443 الموافق 18 ماي2022.

_ المراسيم التنفيذية:

1_ المرسوم التنفيذي رقم 16-267 مؤرخ في 15 محرم عام 1438 الموافق 17 أكتوبر سنة 2016 يعدل المرسوم التنفيذي رقم 06- 348 المؤرخ في 12 رمضان 1427 الموافق 5 أكتوبر سنة 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج العدد 62، مؤرخة في 21 محرم عام 1438 الموافق 23 أكتوبر سنة 2016.

2_ المرسوم التنفيذي رقم 20- 332 المؤرخ في 80 ربيع الثاني عام 1442 الموافق 22 نوفمبر 2020، يحدد كيفيات ممارسة نشاط الإعلام عبر الانترنت ونشر الرد أو التصحيح عبر الموقع الإلكتروني، ج ر ج ج عدد70 الصادرة في 25 نوفمبر 2020.

هـ_ قوانين الدول الأجنبية العربية :

1_ نظام مكافحة جرائم المعلوماتية السعودي، رقم 17 الصادر بتاريخ 03/26/ 2007، الجريدة الرسمية، مجموعة الأنظمة السعودية.

2_ مرسوم بقانون رقم (5) لسنة 2012، بشأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية العدد 540 ملحق السنة الثانية والأربعون، بتاريخ 26-8-2012، الإمارات العربية المتحدة.

3_ قانون رقم (14) لسنة 2014، المتعلق بإصدار قانون مكافحة الجرائم الإلكترونية، الصادر بتاريخ 2014/09/15 الموافق 11/20/ 1435، الجريدة الرسمية القطرية العدد 15، الصادرة بتاريخ 2014/10/02 الموافق 1435/12/08.

4_ قانون الجرائم الإلكترونية الأردني، رقم 27 لسنة 2015، المنشور على الصفحة 5631، من عدد الجريدة الرسمية رقم 5343 بتاريخ 2015/6/1.

5_ قانون رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية المصرية، العدد 32 مكرر (ج)، الصادرة بتاريخ 14 أغسطس سنة 2018.

ثانيا: المراجع باللغة العربية:

1_ الكتب:

أ_ الكتب العامة:

1_ أحسن بوسقيعة، التحقيق القضائي، الطبعة الثانية عشر، دار هومه، الجزائر، 2018.

2_ أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، الجزء الأول، ط 21، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2019.

3_ أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الطبعة الرابعة عشر، دار هومه، للطباعة والنشر والتوزيع، الجزائر، 2014.

4_ بكري يوسف بكري محمد، قانون العقوبات القسم العام النظرية العامة للجريمة، ط1، مكتبة الوفاء القانونية، الاسكندرية، 2013.

5_ عامر خضير حميد الكبيسي، التدريب الإداري والأمني رؤية معاصرة للقرن الحادي والعشرين، ط 1، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية، 2010.

6_ عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، الجزء الأول، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2017/ 2018.

7_ عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام، د.ط، موفم للنشر، الجزائر، 2011.

8_ عبد الله سليمان، شرح قانون العقوبات الجزائري القسم العام، الجزء الأول " الجريمة"، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 2009. .

09_ علي شملال، المستحدث في شرح قانون الإجراءات الجزائية، الكتاب الأول الاستدلال والاتهام، ط 4، دار هومه، الجزائر، 2019-2020.

10_ علي شملال، الجديد في شرح قانون الإجراءات الجزائية، الكتاب الأول الاستدلال والاتهام، ط 3، دار هومه، الجزائر، د.س.ن.

11_ علي شملال، المستحدث في قانون الإجراءات الجزائية الجزائري، الكتاب الثاني التحقيق والمحاكمة، د.ط، دار هومه، الجزائر، د. س. ن.

12_ محمد حزيط، أصول الإجراءات الجزائية في القانون الجزائري، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2018.

13_ محمد محمود سعيد، جرائم غسل الأموال أحكامها الموضوعية وإجراءات ملاحقتها، ط1، دار الفكر العربي، القاهرة، 2007.

14_ نجيمي جمال، قانون حماية الطفل في الجزائر تحليل وتأصيل، ط 2، دار هومه، الجزائر، 2016.

ب_ الكتب المتخصصة:

1_ أحمد عبد اللاه المراغي، الجريمة الإلكترونية ودور القانون الجنائي في الحد منها دراسة تحليلية تأصيلية مقارنة، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2017.

2_ أسامة أحمد المناعسة، جلال محمد الزعبي، جرائم تقنية المعلومات الإلكترونية دراسة مقارنة، ط 3، دار الثقافة للنشر والتوزيع، عمان، 2017.

3_ الطيب بلواضح، الجريمة في الفضاء الإلكتروني في ظل التشريع الجزائري والفرنسي والتشريعات العربية، ط1، دار وائل للنشر والتوزيع، الأردن، 2020.

4_ أمير فرج يوسف، الجريمة المنظمة وعلاقتها بالإتجار بالبشر وتهريب المهاجرين غير الشرعيين والجهود الدولية والمحلية لمكافحتها، ط 1، مكتبة الوفاء القانونية، الإسكندرية، 2015.

5_ بن مكي نجاة، السياسة الجنائية لمكافحة جرائم المعلوماتية، د.ط، دار الخلدونية، الجزائر، 2017.

6_ بهاء المري، جرائم المحمول ووسائل التواصل الاجتماعي فيس بوك- انستجرام- واتسآب- تويتر- فايبر- وحجية الدليل الالكتروني في الاثبات، ط 4، دار الأهرام للنشر والتوزيع والاصدارات القانونية، مصر، 2022.

7_ خالد حسن أحمد لطفي، الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2020.

8_ خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، ط1، دار الفكر الجامعي، الاسكندرية، 2020.

9_ خالد حسن أحمد، الحق في خصوصية البيانات الشخصية بين الحماية القانونية التحديات التقنية – دراسة مقارنة-، د.ط، دار الكتب والدراسات العربية، د. ب. ن، 2020.

10_ خالد ممدوح إبراهيم، الجرائم المعلوماتية، ط 1، دار الفكر الجامعي، الاسكندرية، 2009.

11_ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الاسكندرية، مصر، 2009.

12_ خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر أساليب وثغرات، د ط، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2010.

13_ رامي متولي القاضي، عمر سالم، شرح قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2017 مقارنا بالتشريعات المقارنة والمواثيق الدولية، ط1، مركز الدراسات العربية للنشر والتوزيع، الجيزة، جمهورية مصر العربية، 2020.

14_ زينات طلعت شحادة، الأعمال الجرمية التي تستهدف الأنظمة المعلوماتية، د ط، المنشورات الحقوقية صادر، بيروت، لبنان، د. س. ن.

15_ سامر سلمان الجبوري، جريمة الاحتيال الالكتروني دراسة مقارنة، ط 1، مكتبة زين الحقوقية والأدبية، بيروت، لبنان، 2018.

16_ عبد الاله النوايسية، جرائم تكنولوجيا المعلومات شرح الأحكام الموضوعية في قانون الجرائم الإلكترونية، ط1، دار وائل للنشر والتوزيع، عمان، 2017.

17_ عبد الصبور عبد القوي علي المصري، منال عبد اللاه عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، ط 1، مكتبة القانون والاقتصاد، الرياض، المملكة العربية السعودية، 1433هـ/ 2012.

18_ عبد المجيد لخذاري، الجريمة العالمية الإرهاب نموذجا، ط1، الماهر للطباعة والنشر، سطيف، الجزائر، 2020.

19_ علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة دراسة مقارنة- ، ط 1، منشورات زين الحقوقية، 2013.

20_ علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة – دراسة مقارنة- ، د.ط، المكتب الجامعي الحديث، الاسكندرية، 2019.

21_ عمار عباس الحسيني، جرائم الحاسوب والإنترنت الجرائم المعلوماتية دراسة مقارنة في تشريعات: أمريكا وفرنسا والسويد وإنكلترا والسعودية والسودان، ط 2، منشورات زين الحقوقية، بيروت، لبنان، 2019.

22_ عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، الجزائر، 2021.

23_ غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، منشورات الدار الجزائرية، الجزائر، 2016.

24_ لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، ط 1، دار الحامد، ،الأردن، عمان، 2015.

25_ محمد حماد مرهج الهيتي، الجريمة المعلوماتية نماذج من تطبيقاتها- دراسة مقارنة في التشريع الإماراتي والسعودي والبحريني والقطري والعماني-، دار الكتاب القانوني، دار شتات للنشر والبرمجيات، 2014.

26_ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والقانون المقارن، د ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

27_ محمد سيد عبد الوهاب أبو سريع وشهرته محمد أبو الخير، الدفوع الجنائية في جرائم الأنترنت (الجرائم الالكترونية)، الكتاب الثاني، ط1، دار المحامي للإصدارات القانونية، د. ب. ن، 2022.

28_ محمد نصر محمد، المسؤولية الجنائية لإنتهاك الخصوصية المعلوماتية دراسة مقارنة، مركز الدراسات العربية للنشر والتوزيع، مصر، 2015.

29_ محمود أحمد عبانه، جرائم الحاسوب وأبعادها الدولية، ط1ن دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.

30_ مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت بين القانون الدولي الإتفاقي والقانون الوطني، ط1، مركز الدراسات العربية للنشر والتوزيع، جمهورية مصر العربية، 2016.

31_ مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها) – دراسة مقارنة، دار الخلدونية، الجزائر، 2018.

32_ منى الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية: الهمّ الأمني وحقوق الأفراد، ط1، المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العرب، جامعة الدول العربية، بيروت، لبنان، 2018.

33_ ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، 2018.

34_ نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، 2020.

35_ نعيم مغبغب، مخاطر المعلوماتية والأنترنت – المخاطر على الحياة الخاصة وحمايتها دراسة في القانون المقارن–،د.ط، د.د.ن، د.ب.ن، 1998.

36_ هاني الحبال، قانون المعاملات الإلكترونية والبيانات ذات الطابع الشخصي، ب.د.ن، بيروت، 2019.

37_ هلالي عبد اللاه أحمد، إتفاقية بودابست لمكافحة جرائم المعلوماتية معلقًا عليها، ط1، دار النهضة العربية، القاهرة، 2007.

38_ ياسر محمد الكومي أبو الحطب، الحماية الجنائية والأمنية للتوقيع الإلكتروني، منشأة المعارف، الإسكندرية، 2014.

39_ يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط 1، مطبعة الرمال، (الوادي)، الجزائر، جانفي 2019.

2_أطروحات الدكتوراه ومذكرات الماجستير:

أ_ أطروحات الدكتوراه:

1_ بدري فيصل، مكافحة الجريمة المعلوماتية في القانون الدولي والقانون الداخلي، أطروحة لنيل شهادة دكتوراه علوم –تخصص قانون عام–، كلية الحقوق، جامعة الجزائر01 –بن يوسف بن خدة–، الجزائر، 2017/ 2018.

2_ بلخير محمد آيت عويدة، الضبط الإداري للشبكات الإجتماعية الإلكترونية، أطروحة مقدمة لنيل دكتوراه علوم في الحقوق، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2019/2018.

3_ بن عزة محمد حمزة، المسؤولية القانونية لمتعاملي الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس سيدي بلعباس، الجزائر، 2018/ 2019.

4_ بنور سعاد، حماية الحياة الخاصة للعامل، أطروحة للحصول على شهادة دكتوراه في العلوم في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة وهران2، الجزائر 2017/2016.

5_ حايطي فاطيمة، إجراءات التحقيق في الجرائم الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، الجزائر، 2022-2023.

6_ حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة لنيل شهادة الدكتوراه ل.م.د في القانون العام تخصص قانون جنائي وعلم الإجرام، كلية الحقوق، جامعة الجزائر1، الجزائر، 14 سبتمبر 2020.

7_ ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، 2015-2016.

8_ سوماتي شريفة، السياسة الجنائية للمشرع الجزائري في مواجهة الجريمة المستحدثة، رسالة لنيل شهادة دكتوراه علوم، كلية الحقوق، جامعة الجزائر 1، الجزائر،2017- 2018.

9_ سي ناصر محمد، التعاون الجزائري الدولي في مجال مكافحة الجريمة الدولية والجريمة المنظمة وتعقب المذنبين، أطروحة لنيل شهادة الدكتوراه في حقوق الإنسان والحريات، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عمار ثليجي الأغواط، الجزائر، 2021-2022.

10_ عفاف خذيري، الحماية الجنائية للمعطيات الرقمية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي–تبسة– ، الجزائر، 2017/ 2018.

11_ قطاوي أمال، نطاق تطبيق مبدأ الإختصاص الجنائي العالمي، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون العام، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد إبن باديس مستغانم، الجزائر، نوقشت بتاريخ 2021/03/09.

12_ لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، 2020– 2021.

13_ محمد الصغير سليني، قرارات المنظمات الدولية ودورها في إرساء قواعد القانون الدولي، أطروحة لنيل شهادة دكتوراه علوم في الحقوق، كلية الحقوق والعلوم السياسية، جامعة يحي فارس بالمدية، نوقشت بتاريخ 2021/02/01، ص135– 136.

14_ يزيد بوحليط، السياسة الجنائية في مجال الجرائم الالكترونية، أطروحة لنيل شهادة دكتوراه العلوم، كلية الحقوق، جامعة باجي مختار، عنابة، الجزائر، 2016.

ب_ رسائل الماجستير:

1_ إبراهيم محمد القاسمي، جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات الإلكترونية (وفقا للمرسوم بقانون رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات وتعديلاته)، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون العام، جامعة الإمارات العربية المتحدة، كلية القانون، نوفمبر 2018.

2_ أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيات الإعلام والإتصال في ضوء القانون رقم 04/09، مذكرة مقدمة لنيل شهادة الماجستير ، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، الجزائر، 2013/2012.

3_ إكرام سليمان قجم، الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والقانون المقارن، رسالة قُدمت استكمالا لمتطلبات كلية القانون للحصول على درجة الماجستير في القانون الخاص، جامعة قطر، كلية القانون، يونيو 2021.

4_ محمد منصور البابا، تجريم الشائعة في التشريع الأردني (دراسة مقارنة)، قدمت هذه الرسالة إستكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، كلية الحقوق، حزيران 2020.

5_ مصطفى جمال حنفي زينو، دور الضبط الإداري في مجال الجرائم الإلكترونية المخلة بالأمن العام (دراسة تحليلية)، قدمت هذه الرسالة إستكمالا لمتطلبات الحصول على درجة الماجيستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الأزهر غزة، فلسطين، 1439هـ، الموافق ل2017.

6_ ملاوي قدور، التعاون الدولي في مكافحة الجريمة المنظمة، رسالة ماجستير القانون الجنائي الدولي، كلية الحقوق والعلوم السياسية جامعة البليدة 2، 2017.

3_ المقالات:

1_ ابراهيم بن سليمان الحربي، الجريمة الدولية بين القانون الداخلي والقانون الوطني، دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، المجلد 6، العدد 14، مارس (آذار) 2014.

2_ أحمد لطفي السيد مرعي، الولاية الجنائية العالمية(دراسة مقارنة)، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، مصر، (الجزء الأول)، المجلد 11، العدد 76، يونيو 2021.

3_ إدريس قرفي، تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية: بين إتفاقية بودابست والتشريع الجزائري، مجلة الحقوق والحريات، العدد 2، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، 2014.

4_ أسامة حسين محي الدين عبد العال، تجريم الشائعات عبر وسائل التواصل الاجتماعي في التشريع الجنائي المصري دراسة تحليلية، مجلة العلوم الإقتصادية والقانونية، كلية الحقوق، جامعة عين الشمس، مصر، العدد 1، السنة 63، يناير "ج 1" 2021.

5_ العنكبي نزار، نحو قانون جنائي دولي لجرائم المعلوماتية والأنترنت ذات الصفة الدولية، مجلة العلوم القانونية والسياسية، الجمعية العلمية للبحوث والراسات الاستراتيجية، المجلد 3، العدد 5، حزيران– كانون الثاني 2013.

6_ العيداني محمد، يوسف زروق، حماية المعطيات الشخصية في الجزائر على ضوء القانون 18-07 (المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي)، مجلة معالم للدراسات القانونية والسياسية، المركز الجامعي، علي كافي، تندوف، الجزائر، العدد 05، ديسمبر 2018.

7_ إلهام بن خليفة، التفتيش كإجراء تقليدي لجمع أدلة الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، المجلة القانونية للبحوث القانونية والسياسية، جامعة الوادي، الجزائر، المجلد 2، العدد 1، 2018.

8_ آمال بوبكر، التصديق الالكتروني في النظام القانوني الجزائري، مجلة المفكر للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، العدد3، سبتمبر 2018.

9_ أمحمدي بوزينة آمنة، خصوصية قواعد التجريم عن الإعتداء على أنظمة المعالجة الآلية للمعطيات في إطار التشريع الجزائري، مجلة ببليوفيليا لدراسات المكتبات والمعلومات، مخبر الدراسات في الرقمنة وصناعة المعلومات الالكترونية بالمكتبات الأرشيف والتوثيق، جامعة العربي التبسي، تبسة، الجزائر، العدد 05، 2020.

10_ أميمة خديجة حميدي، إمكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية، مجلة الحقوق والحريات، مخبر الحقوق والحريات في الأنظمة المقارنة، جامعة بسكرة، الجزائر، المجلد 10، العدد 01، 2022.

11_ بارة سمير الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الإنساني، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1 الحاج لخضر، باتنة، الجزائر، العدد 4، جويلية 2017.

12_ بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة، الجزائر، المجلد أ، العدد 50، ديسمبر 2018.

13_ برقوق يوسف، المساعدة القضائية المتبادلة لمواجهة الجرائم الإلكترونية، مجلة البصائر للدراسات القانونية والإقتصادية، كلية الحقوق، جامعة بوشعيب بلحاج عين تموشنت، الجزائر، المجلد 01، العدد01، 2021.

14_ بطيحي نسمة، الجرائم المتعلقة بانتهاك الأحكام الإجرائية المقررة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، كتاب جماعي خاص بالملتقى الدولي المحكم الخصوصية في مجتمع المعلومات، طرابلس بين 19- 20 /07/ 2019، مركز جيل البحث، العام السابع، العدد 26، لبنان، يوليو 2019.

15_ بطيحي نسمة، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي، مجلة الفقه القانوني والسياسي، مخبر الدراسات القانونية، جامعة ابن خلدون تيارت، الجزائر، المجلد 01، العدد 01، 2019.

16_ بن سليمان محمد الأمين، خلفي عبد الرحمان، الإجراءات الإستثنائية في جرائم الفساد على ضوء القانون الإجرائي الجزائي الجزائري، مجلة الدراسات حول فعلية القاعدة القانونية، مخبر البحث حول فعلية القاعدة القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، المجلد 04، العدد01، 2020.

17_ بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي سعيدة، الجزائر، العدد6، جوان 2016.

18_ بن يوسف القينعي، الجرائم المتعلقة بالإستغلال غير المشروع للمعطيات الشخصية على ضوء القانون: 18-07، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الانسانية والاجتماعية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 4، جويلية 2021.

19_ بوقرة جمال الدين، عنان جمال الدين، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوالضياف، المسيلة، الجزائر، المجلد 07، العدد 01، جوان 2022.

20_ بوكر رشيدة، الدخول أو البقاء داخل نظم معلومات المؤسسة الإقتصادية " بين عدم التصريح والحماية الجزائية"، مجلة قانون العمل والتشغيل، مخبر قانون العمل والتشغيل، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، الجزائر، المجلد 06، العدد 01، جانفي 2021.

21_ تبينة حكيم، آليات الضبط الإداري لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة، الجزائر، المجلد 58، العدد 01، 2021.

22_ تومي يحي، الحماية القانونية للمعطيات ذات الطابع الشخصي على ضوء القانون رقم 18-07 دراسة تحليلية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 04، العدد 02، السنة 2019.

23_ جمال زين العابدين أمين أحمد، الإختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية "دراسة مقارنة"، مجلة مستقبل العلوم الإجتماعية، الجمعية العامة العربية للتنمية البشرية والبيئية، مصر، العدد الرابع، يناير 2021.

24_ جيلالي الحسين، التعاون الجنائي الدولي في مكافحة الجريمة العالمية، مجلة القانون، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد زبانة بغليزان، الجزائر، المجلد07، العدد02، 2018.

25_ حابت أمال، دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، المجلة الدولية للبحوث القانونية والسياسية، مخبر السياسات العامة وتحسين الخدمة العمومية بالجزائر، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 05، العدد 03، ديسمبر 2021.

26_ حديدان سفيان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 2، العدد 8، ديسمبر 2017.

27_ حزام فتيحة، الضمانات القانونية لمعالجة المعطيات ذات الطابع الشخصي دراسة على ضوء القانون رقم 18-07، مجلة الاجتهاد للدراسات القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي، تامنغست، الجزائر، المجلد 08، العدد 04، 2019.

28_ حزام فتيحة، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية قراءة في أحكام المرسوم الرئاسي رقم 20-05، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 13، العدد 3، أكتوبر 2020، ص181.

29_ حزيط محمد، الإختصاصات الإستثنائية المخولة لجهات المتابعة والتحقيق بشأن جرائم الفساد في القانون الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 05، العدد 02، 2020.

30- حسون عبيد هجيج، حسن مهدي حمزة، جريمة بث الأخبار والإشاعات الكاذبة، مجلة جامعة بابل للعلوم الانسانية، جامعة بابل، العراق، المجلد26، العدد 7، سبتمبر/ أيلول 2018.

31_ حسين جيجة، سحواد نسيمة، جهود استباقية للأمن الوطني لتحقيق الأمن المعلوماتي والامتياز في الأداء، المديرية العامة للأمن الوطني، العدد 129، ديسمبر 2015.

32_ حنان المساوي، إثبات جريمة السرقة المعلوماتية والقانون الواجب التطبيق، مجلة الأبحاث والدراسات القانونية، المركز المغربي للدراسات والإستشارات القانونية وحل المنازعات، المغرب، العدد 4، نونبر – دجنبر، 2014.

33_ خرشي إلهام، النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، مجلة الأبحاث القانونية والسياسية، مخبر دراسات وأبحاث حول المجازر الاستعمارية ومخبر تطبيقات التكنولوجيا الحديثة على القانون، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف، الجزائر، المجلد 04، العدد 01، 2022.

34_ خرشي عثمان، عمارة فتيحة، تسليم المجرمين كآلية دولية لمكافحة الجرائم المعلوماتية، مجلة البحوث القانونية والسياسية، جامعة سعيدة الدكتور مولاي طاهر، الجزائر، المجلد 02، العدد 10، جوان 2018.

35_ خلافي سفيان، مفهوم الولاية العالمية للمحاكم الجنائية الوطنية، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق، جامعة مولود معمري تيزي وزو، الجزائر، العدد2، 2012.

36_ خلفي عبد الرحمان، عثماني بلال، حماية الرعايا الجزائريين بالخارج في إطار القانون الجنائي الوطني، مجلة الدراسات حول فعلية القاعدة القانونية، مخبر البحث حول فعلية القاعدة القانونية، جامعة عبد الرحمان ميرة بجاية، الجزائر، المجلد 03، العدد01، 2019.

37_ خليفي محمد، إشكالية الإختصاص القضائي الدولي في مكافحة الجريمة المعلوماتية، مجلة الميزان، مخبر الجرائم العابرة للحدود، معهد الحقوق والعلوم السياسية، المركز الجامعي صالح أحمد بالنعامة، الجزائر، العدد1، ديسمبر 2016.

38_ خواثرة سامية، خواثرة سامية، المبادئ الأساسية لحماية البيانات الشخصية بين الجهود الدولية والتشريع الجزائري، مجلة الدراسات القانونية والبحوث الانسانية، كلية العلوم الانسانية والاجتماعية، جامعة العربي التبسي، تبسة، الجزائر، المجلد 07، العدد03، ماي 2022.

39_ دنيا عبد العزيز فهمي، المسؤولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي، مجلة الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الاسكندرية، مصر، المجلد 2، العدد 2، يوليو .2019

40_ رابح لهوى، الإشكاليات العملية الهامة للتفتيش الإلكتروني –دراسة مقارنة– الجزء الأول: إشكالية المفهوم والتكييف، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 06، العدد 02، 2020.

41_ رابح نهائلي، قيرة سعاد، دور المنظمات الدولية في مكافحة الجريمة المنظمة (منظمة الأمم المتحدة، المنظمة الدولية للشرطة الجنائية نموذجا)، مجلة البحوث القانونية والإقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي آفلو، الجزائر، المجلد 04، العدد02، 2021.

42_ ربيعة فرحي، أثر الجائحة كوفيد–19 في سياسة التجريم والعقاب في قانون العقوبات الجزائري، المجلة الجزائرية للعلوم القانونية والسياسية، جامعة بن يوسف بن خدة، الجزائر، المجلد 58، العدد03، 2021.

43_ ربيعة فرحي، المساعدة القانونية المتبادلة كآلية للتعاون الدوليالأساس القانوني ومعقوقات التفعيل، مجلة المفكر للدراسات القانونية والسياسية، جامعة الجيلالي بونعامة خميس مليانة، الجزائر، المجلد 3، العدد4، ديسمبر 2020.

44_ رجاء أومدور، التفتيش الجزائي في البيئة الإفتراضية، مجلة صوت القانون، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد07، العدد 01، ماي 2020.

45_ رضا بو الجدري، وردة سالمي، سلطة ضبط البريد والاتصالات الالكترونية قراءة في المهام والصلاحيات من خلال أحكام القانون 18-04، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، الجزائر، المجلد 34، العدد 1، جامعة الإخوة منتوري قسنطينة 1، الجزائر، 2023.

46_ رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الوادي، الجزائر، العدد5 ، جوان 2012.

47_ زراري نسرين، بوقرة إسماعيل، الرقم الأسود في الجرائم المتعلقة بأنظمة معالجة المعطيات، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، المجلد 09، العدد 01، 2022.

48_ زراري نسرين، بوقرة اسماعيل، نحو التحول إلى المحكمة الرقمية، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، المجلد 10، العدد 02، 2023.

49_ سارة محمد، التعاون الدولي في تسليم المجرمين في ضوء التشريعات الوطنية والاتفاقيات الدولية، مجلة جامعة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد17، العدد 1، يونيو 2020.

50_ سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا « دراسة مقارنة»، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين الشمس، مصر، المجلد62، العدد 1، جانفي 2020.

51_ سورية ديش، أنواع الجرائم الإلكترونية وإجراءات مكافحتها، المركز الديمقراطي العربي، مجلة العلوم السياسية والقانون، العدد 1، 2017.

52_ شريفة كلاع، ظاهرة تجنيد الشباب في الجماعات الإرهابية من خلال استخدام شبكات التواصل الاجتماعي، مجلة مدارات سياسية، مركز المدار المعرفي للأبحاث والدراسات، الجزائر، المجلد 2، العدد السادس، سبتمر 2018.

53_ شريفة سوماتي، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال كآلية جديدة ضمن الجهاز القضائي المتخصص، مجلة الدراسات القانونية، مخبر السيادة والعولمة، جامعة يحي فارس، المدية، الجزائر، المجلد08، العدد02، جوان 2022.

54_ شنه محمد، جريمة نشر الأخبار الكاذبة في التشريع الجزائري، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر، المجلد 07، العدد01، جوان 2022.

55_ شوقي يعيش تمام، عزيزة شبري، تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية، مجلة الاجتهاد القضائي، مخبر أثر الإجتهاد القضائي على حركة التشريع، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد 15، سبتمبر .2017

56_ شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، جامعة الشارقة، الشارقة، الإمارات العربية المتحدة، المجلد 17، العدد1، شوال 1441/ يونيو 2020.

57_ عائشة عبد الحميد، الإطار القانوني للترصد الإلكتروني الوقائي كإطار للإصلاح القضائي في الجزائر، مجلة التراث، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 11، العدد 05، ديسمبر 2021.

58_ عبد الرزاق طلال جاسم، الحاجة إلى تحديث اليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، مجلة جامعة تكريت للحقوق، العراق، المجلد5، العدد1، الجزء2، 2020.

59_ عبد العزيز لزعر، رشيد زياني، آلية الاتحاد الافريقي للتعاون الشرطي (الأفريبول) ودورها في مكافحة الجريمة الإلكترونية، مجلة متون، كلية العلوم الاجتماعية والإنسانية، جامعة الدكتور مولاي الطاهر سعيدة، الجزائر، المجلد 13، العدد3، سبتمبر 2021.

60_ عبد الفتاح قادري، حيدرة سعدي، آليات عمل الأقطاب الجزائية المتخصصة في جرائم الفساد، مجلة العلوم الإنسانية لجامعة أم البواقي، جامعة العربي بن مهيدي، أم البواقي، الجزائر، المجلد8، العدد1، مارس 2021.

61_ عبد المومن بن صغير، تطبيق النص الجنائي بين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية بجامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 10، العدد03، ديسمبر 2019.

62_ عراب مريم، الإختصاص القضائي في الجريمة المعلوماتية، حوليات كلية الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة وهران، الجزائر، المجلد 07، العدد03، ديسمبر 2015.

63_ عز الدين عثماني، إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الإتصال والمعلوماتية، مجلة دائرة البحوث القانونية والسياسية– مخبر المؤسسات الدستورية والنظم السياسية، العدد 4، جانفي 2018.

64_ عز الدين عثماني، صور الركن المادي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، الجزائر، المجلد 09، العدد 03، ديسمبر 2018.

65_ عصموني خليفة، مكانة قرارات المنظمات الدولية بين مصادر القانون الدولي العام، مجلة السياسة العالمية، مخبر الدراسات السياسية والدولية، جامعة امحمد بوقرة بومرداس، الجزائر، المجلد 05، العدد02، 2021.

66_ عطابة زهية، المساهمة التشريعية لمنظمة التعاون والتنمية الاقتصادية في التنمية الاقتصادية، دفاتر البحوث العلمية، المركز الجامعي تيبازة، الجزائر، المجلد 5، العدد 11، ديسمبر 2017.

67_ عفيري عقيلة، عمارة هدى، مبدأ تسليم المجرمين كإجراء لتكريس العدالة الجنائية الدولية، مجلة دراسات وأبحاث المجلة العربية في العلوم الإنسانية والاجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد 12، العدد4، 2020.

68_ علواش فريد، التعاون الدولي عن طريق نظامي تسليم المجرمين والتسليم المراقب، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، المجلد 12، العدد 14، 2017.

69_ فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، العدد2، 2015.

70_ فاطمة الوحش، لهذه الأسباب انتشر خطاب الكراهية عبر مواقع التواصل، مقال منشور على الرابط التالي:

http://www.ech-chaab.com/ar/%D8%A3%D8%B9%D9%85%D8%AF%D8%A9-%D9%88-%D9%85%D9%82%D8%A7%D9%84%D8%A7%D8%AA/%D8%AD%D9%88%D8%A7%D8%B1%D8%A7%D8%AA/item/186619-%D9%84%D9%87%D8%B0%D9%87-

71_ فتيحة حزام، إجراءات المعالجة الآلية للمعطيات ذات الطابع الشخصي وفقا لأحكام القانون 18-07، مجلة البحوث والدراسات الإنسانية، جامعة 20 أوت 1955، سكيكدة، الجزائر، المجلد 15، العدد 01، 2021.

72_ فريد صحراوي، مكافحة خطاب الكراهية في البيئة الرقمية دراسة على ضوء القانون 20-05، دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي مرسلي عبد الله، تيبازة، الجزائر، المجلد 06، العدد 01، 2022.

73_ فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة منتوري، قسنطينة، الجزائر، العدد 33، جوان 2010.

74_ قسمية محمد، خضري حمزة، مكافحة الجرائم الماسة بنظام المعالجة الآلية للمعلومات في قانون العقوبات الجزائري، مجلة صوت القانون، مخبر نظام الحالة المدنية، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، المجلد 07، العدد 02، نوفمبر 2020.

75_ كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية لقانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد 2 ، ديسمبر 2020.

76_ كحلاوي عبد الهادي، بن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، معهد الحقوق والعلوم السياسية، المركز الجامعي صالحي أحمد، النعامة، الجزائر، المجلد 07، العدد 02، 2021.

77_ كعرار سفيان، الآليات المؤسساتية الأوروبية لمكافحة الجريمة المنظمة عبر الوطن، المجلة الأكاديمية للبحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الأغواط، الجزائر، المجلد الرابع، العدد الأول، 2020.

78_ كمال بوبعاية، السعيد برابح، التدريب ودوره في مكافحة الجريمة المنظمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، مخبر الدراسات والبحوث في القانون والأسرة والتنمية الإدارية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، الجزائر، المجلد 6، العدد2، 2021.

79_ كمال بوبعاية، مبروك لمشونشي، الحماية القانونية الدولية للمعطيات الشخصية في البيئة الافتراضية، مجلة الدراسات القانونية والسياسية، جامعة طاهر مولاي سعيدة، الجزائر، المجلد 07، العدد01، جانفي 2021.

80_كهينة سلام، جميلة قادم، الضبط الإعلامي في التشريع الجزائري قراءة في مهام، صلاحيات وخصائص سلطة ضبط السمعي البصري وفق القانون 14-04 المنظم للنشاط

السمعي بصري، مجلة الرسالة للدراسات الاعلامية، كلية العلوم الانسانية والاجتماعية ، جامعة العربي التبسي، تبسة، الجزائر، المجلد 06، العدد 02، جوان 2022.

81_ كهينة قونان، نوارة حمليل، السلطة الوطنية كهيئة مكلفة برقابة احترام تطبيق قانون حماية المعطيات الشخصية رقم 18-07، مجلة الدراسات القانونية، مخبر السيادة والعولمة، كلية الحقوق والعلوم السياسية، جامعة يحى فارس، المدية، الجزائر، المجلد 07، العدد02، جوان 2021.

82_ لخضر القيزي، الشروط الموضوعية لتسليم المجرمين، مجلة العلوم الإنسانية لجامعة أم لبواقي، جامعة العربي بن مهيدي أم البواقي، الجزائر، المجلد 07، العدد02، جوان 2020.

83_ ليلى الجنابي، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، 1438-2017، مقال منشور على الرابط التالي:

https://www.ahewar.org/debat/show.art.asp?aid=571423

84_ ليندة شرابشة، السياسة الدولية والإقليمية في مجال مكافحة الجريمة الإلكترونية. الاتجاهات الدولية في مكافحة الجريمة الالكترونية، دراسات وأبحاث، جامعة زيان عاشور الجلفة، الجزائر، المجلد1، العدد 1، 2009.

85_ مانع سلمى، التفتيش كإجراء للتحقيق في الجرائم المعلوماتية، مجلة العلوم الإنسانية- جامعة محمد خيضر بسكرة، العدد 22، جوان 2011.

86_ مبخوتة أحمد، القيمة القانونية للقرارات والتوصيات الصادرة عن الجمعية على ضوء أحكام القانون الدولي المعاصر، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة، الجزائر، المجلد 3، العدد 1، 2010.

87_ مبخوتة أحمد، الوظيفة التشريعية للجمعية العامة وأثرها على تطور قواعد القانون الدولي المعاصر، مجلة القانون، معهد العلوم القانونية والادارية، المركز الجامعي أحمد زبانة بغليزان، الجزائر، المجلد 07، العدد 02، 2018.

88_ محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة– بجاية، الجزائر، المجلد 14، العدد02، 2016.

89_ محمد أحمد عبد الرحمن طه، النظام القانوني لتسليم المجرمين مصادر وأنزاع التسليم، دراسات قانونية، مركز البصيرة للبحوث والاستشارات والخدمات التعليمية، الجزائر، العدد7، ماي 2010.

90_ محمد السعيد تركي، نسيغة فيصل، سياسة الوقاية والمنع من الجريمة، مجلة البحوث والدراسات، جامعة حمه لخضر، الوادي، الجزائر، المجلد 15، العدد01، شتاء 2018.

91_ محمد السيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، 2006، مقال منشور على الرابط التالي:
https://down.ketabpedia.com/files/bkb/bkb-ab01080-ketabpedia.com.pdf.

92_ محمد بن علي كومان، أخبار مجلس وزراء الداخلية العرب، فريق من الخبراء العرب يعقدون لقاءهم الأول في جامعة نايف لمواجهة الجرائم الالكترونية، مجلة الأمن والحياة، جامعة نايف العربية تدعو لتبني إستراتيجية للحد من حرائق الغابات، العدد 442، أبريل– يونيو 2022.

93_ محمد نصر القطري، آليات التعاون الدولي لتسليم المجرمين وآثاره في الحد من الجرائم المستحدثة، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، المجلد 35، العدد3، 2019.

94_ مراد مشوش، الجهود الدولية لمكافحة الإجرام السيبراني، مجلة الواحات للبحوث والدراسات، جامعة غرداية، الجزائر، المجلد 12، العدد2، 2019.

95_ مرو رياض علي أبو ظريس، مراد عبد الله المواجدة، أشكال خطاب الكراهية على مواقع التواصل الاجتماعي في المجتمع الأردني من وجهة نظر العاملين في وحدة مكافحة الجرائم الالكترونية، مجلة التربية، جامعة الأزهر كلية التربية بالقاهرة، مصر، العدد 189، الجزء الخامس، يناير 2021.

96_ مريم لوكال، الحماية القانونية الدولية والوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمة لخضر الواد، الجزائر، المجلد10، العدد01، أفريل 2019.

97_ مشتة نسرين، بن عبيد إخلاص، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، معهد العلوم القانونية والإدارية، المركز الجامعي أحمد بن يحي الونشريسي، تيسمسيلت، الجزائر، المجلد 06، العدد 01، 2021.

98_ مصطفى عبد الباقي، التحقيق في الجريمة الإلكترونية وإثباتها في فلسطين: دراسة مقارنة، دراسات، علوم الشريعة والقانون، المجلد 45، العدد4، ملحق 2، 2018.

99_ مصطفى هنشور وسيمة، النظام القانوني لمقدمي خدمات الإنترنت في التشريع الجزائري، مجلة البحوث القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الطاهر مولاي، سعيدة، الجزائر، العدد 5، ديسمبر 2015.

100_ ملياني عبد الوهاب، الجرائم الماسة بالمعطيات الشخصية على ضوء القانون رقم 07/18، مجلة البحوث القانونية والاقتصادية، معهد الحقوق والعلوم السياسية، المركز الجامعي أفلو، أفلو، الجزائر، المجلد 06، العدد 01، 2023.

101_ ممدوح حسن مانع العدوان، نادر عبد الحليم السلامات، مشروعية وحجية الدليل الالكتروني في التشريع الجزائي الأردني، دراسات: علوم الشريعة والقانون، الجامعة الأردنية عمادة البحث العلمي، الأردن، المجلد 45، العدد 4، ملحق 2، 31 ديسمبر/ كانون الأول 2018.

102_ منال مروان منجد، جرائم الكراهية: دراسة تحليلية مقارنة، مجلة جامعة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد 15، العدد1، يونيو 2018.

103_ نبيل لحمر، الأخبار الكاذبة عبر شبكات التواصل الاجتماعي وآثارها على إتجاهات الرأي العام دراسة في المفهوم، العلاقة والأهداف، مجلة الباحث للدراسات الأكاديمية، كلية الحقوق والعلوم السياسية، جامعة باتنة 11 الحاج لخضر، باتنة، الجزائر، المجلد 07، العدد02، جوان 2020.

104_ نبيلة رزاقي، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي –دراسة مقارنة–، مجلة الدراسات القانونية المقارنة، مخبر البحث، "القانون الخاص المقارن"، جامعة حسيبة بن بوعلي، الشلف، الجزائر، المجلد 07، العدد01، 2020، ص .1999

105_ نزيه محمد على عبد الغني، تداول المعلومات في الحد من آثار الشائعات على ضوء التشريعات الدولية والوطنية، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين الشمس، مصر، العدد 1، السنة 63، يناير الجزء 2021.

106_ نسيب نجيب، آليات التعاون القانوني الدولي في مكافحة الجريمة المنظمة، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، العدد1، 2019.

107_ نعمان كريمة، الشرطة الجزائرية تتصدى لصناع الكراهية عبر المنصات الرقمية، مجلة إعلامية أمنية، تصدر عن المديرية العامة للأمن الوطني، العدد 149، أكتوبر 2021.

108_ هشام بخوش، الجرائم الماسة بسلامة المعطيات ذات الطابع الشخصي وفقا للقانون 18-07 معالجة معطيات فيروس كورونا _ نموذجا، مجلة أبحاث قانونية وسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد الصديق بن يحي، جيجل، الجزائر، المجلد 06، العدد 01، جوان 2021.

109_ وليد عبد الله سالم ال علي، مدى إنعقاد الإختصاص للقضاء الإماراتي بنظر أشد الجرائم الدولية الخطيرة وفقا لمبدأ الإختصاص الجنائي العالمي، مجلة الشارقة للعلوم القانونية، الشارقة، الإمارات العربية المتحدة، المجلد 19، العدد1، مارس .2022

110_ يزيد بوحليط، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري، التواصل في الاقتصاد والادارة والقانون، جامعة باجي مختار عنابة، الجزائر، العدد 48، ديسمبر 2016.

4_ المؤتمرات والملتقيات:

1_ بن عمیور أمینة، بوحلایس إلهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، عدد خاص بفعاليات الملتقى الدولي: " القانون الجنائي للأعمال نحو توجه جديد للتجريم المنعقد يوم 21 أكتوبر 2021 عبر التحاضر المرئي عن بعدZOOM، مجلة البحوث في العقود وقانون الأعمال، مخبر العقود وقانون الأعمال، جامعة الإخوة منتوري قسنطينة1، قسنطينة، الجزائر، المجلد 07، العدد 01، 2022.

2_ حملاوي عبد الرحمن، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، المنعقد بتاريخ 16-17 نوفمبر 2015، جامعة بسكرة، الجزائر.

3_ محمد حبحب، تطبيق القواعد الجزائية الإجرائية على الجريمة الإلكترونية: تحديات وآفاق، مجلة كلية القانون الكويتية العالمية، كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس، ملحق خاص، المجلد 6، العدد 3، الجزء الأول، 9- 10 مايو 2018م شعبان 1439.

4_ وائل محمد نصيرات، الجهود الدولية في مكافحة الجرائم المعلوماتية والصعوبات التي تواجهها، المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC، جامعة الإمام محمد بن سعود الإسلامية- كلية علوم الحاسب والمعلومات، الرياض، المملكة العربية السعودية، نوفمبر 2015.

مقال منشور على الرابط التالي: http://search.mandumah.com/Record/690618

5_ وردة شرف الدين، التعاون القضائي والقانوني لمكافحة جريمة غسيل الأموال والمرتكبة بواسطة تقنية المعلومات وفقا للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، عدد خاص بأشغال الملتقى الدولي حول: آليات مكافحة جرائم الفساد في التشريعات المغاربية، منعقد بتاريخ 04/ 05 ديسمبر 2018، منشور بمجلة الباحث للدراسات الأكاديمية، المجلد 08، العدد 02، 2021.

5_ المنشورات والتقارير:

1_ تقرير للإنتربول يحذر من أن الجريمة الإلكترونية في أفريقيا تشكل تهديدا أشد خطرا من أيّ وقت مضى، 14 أغسطس، 2020.

6_ المعاجم والقواميس:

1_ قاموس المصطلحات المستعملة في الجريمة المعلوماتية، مركز البحوث القانونية والقضائية، وزارة العدل، الجزائر.

2_ معجم المعاني الجامع– معجم إلكتروني عربي عربي: https://www.almaany.com /

7_المواقع الالكترونية باللغة العربية:

1_ الموقع الرسمي للانتربول:https://www.interpol.int

2_ الموقع الرسمي لليوروجيست: https://www.eurojust.europa.eu

3_ الموقع الرسمي للأفريبول: https://afripol.africa-union.org

4_ الموقع الرسمي لمجلس وزراء الداخلية العرب: https://www.aim-council.org

5_الموقع الرسمي للمنظمة العربية لتكنولوجيا الاتصال والمعلومات: http://www.aicto.org

6_ الموقع الرسمي لجامعة نايف العربية للعلوم الأمنية: https://nauss.edu.sa

7_ الموقع الرسمي للأوروبول: https://www.europol.europa.eu/

8_ الموقع الرسمي للمديرية العامة للأمن الوطني: https://www.algeriepolice.dz

9_ الموقع الرسمي لقيادة الدرك الوطني: https://www.mdn.dz

10_الموقع الرسمي للسلطة الوطنية لحماية المعطيات الشخصية: https://anpdp.dz

11_ موسوعة ويكيبيديا: https://ar.wikipedia.org

المصادر والمراجع باللغة الأجنبية:

أولا: المصادر باللغة الأجنبية:

1_ الاتفاقيات الدولية:

1_la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne, Série des traités européens - n° 108 , Conseil de l' Europe, Strasbourg, 28.I.1981.
2 _Convention sur la cybercriminalité, Conseil de L' Europe, Série des traités européens - n° 185, Budapest, 23.XI.2001.
3_ Instrument Juridique de l'Union Africaine, convention de l'union africaine sur la cyber sécurité et la protection des données à caractère personnel, Adopté par la 23ème Session Ordinaire de la Conférence de l'Union à Malabo, le 27 juin 2014, document U.A N : EX.CL/846(XXV).
4_Manuel de droit européen en matière de protection des données, Édition 2018 **European.**

2_ البروتوكولات:

1_ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, European Treaty Series - No. 189, Conseil of L'Europe, Strasbourg, 28.I.2003. https://rm.coe.int/168008160f

3_ اللوائح:

1_ RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel de l'Union européenne.

4_ التوصيات:

1_OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, Legal Instruments, 2022.

5_ القوانين الداخلية:

1_ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

2_ Loi n°88-19 du 05 janvier 1988, relative à la fraude l'informatique, JORF du 06 janvier 1988 , (LOI GODFRAIN).

3_Loi n° 2004/575 du 21 juin 2004, pour la confiance dans léconomie numérique JORGE n 143 du 22 juin page 11168 texte n 02.
4_ loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

ثانيا: المراجع باللغة الأجنبية:

1_ الكتب باللغة الأجنبية:

1_Alain Bensoussan, L'informatique et le droit ,tome 2, edition Hermés, paris 1994.
2_ Brigitte van dorsselaere , Guide juridique de l'informatique, Aubin imprimeur, Paris ,France,1990.
3_ Alain Hollande, Prartique du droit de l'informatique et de l'internet, sixéme édition, éditions delmas, Belgique, 2008 .

4_Cesare Parodi, Valentina Sellaroli, DIRITTO PENALE DE LL'INFORMATICA, REATI DELLA RETE E SULLA RETE, Giuffré Francis lefebvre, Milano, 2020.

5_ Guillaume champy, LA FRAUDE INFORMATIQUE , tome 1, presses universitaires d'aix-marseille , marseille ,1992.

6_ G. URICCHIO, *Il Cyberterrorismo*, in M. IASELLI (a cura di), *Investigazioni digitali*, Giuffrè Francis Lefebvre, Milano, 2020.

2_ الأطروحات والرسائل باللغة الأجنبية:

1_ Romain BOOS, La lutte Contre La cybercriminalité Au Regard De L'action Des états, Doctorat De Droit privé Et sciences Criminelles, Université De Lorraine, 2016.
2_ Guy Marcel KAMENI, la vie privée en droit camerounais, thése en vue de l'obtention du doctorat, l`université de toulouse 1 capitole (UT1 capitole) EA1920 en cotutelle internationale avec:l`université de douala (cameroun), 2012/2013 .

3_ المقالات:

1_ Wassila Kannoufi , Protection des données à caractère personnel: Un cadre juridique en évolution Protection of Personal Data: An Evolving Legal Framework, Journal of letters and Social Sciences, Vol 19, N° 02 , 2022 .
2_Cristos Velasco, Cybercrime and Artificial Intelligence.An overview of the work of international organizations on criminal justice and the international applicable instruments, Journal of the Academy of European La, Vol 23, issue 1, May 2022.
3_ DEHBI Abdelhakim , Cybersecurity in Africa: Challenges and measures, WORLD POLITICS , Volume (6), N°(2), 2022.

4_ Jan Kleijssen and Pierluigi Perri , Chapter 7 Cybercrime, Evidence and Territoriality: Issues and Options, Law 2016, Netherlands Yearbook of International Law 47, 2017.

5_ Myriam QUÉMÉNER, Yves CHARPENEL« Cybercriminalité, Droit pénal appliqué», 2010, ECONOMICA ,Paris France, 2010 .
6_ Orin S. Kerr, Fourth Amendment Seizures of Computer Data, Yale Law Journal, Vol. 119, Issue 4, (2010).
7_ Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, Michigan Telecommunications and Technology Law Review, Vol. 8, Issue 39, (2002).

8_ Susan W. Brenner , Bert-Jaap Koops, Approaches to Cybercrime Jurisdiction**,** Journal of High Technology Law, Vol. IV No. 1, 2004.

9_ Vendius, Trine Thygesen , Europol's Cybercrime Centre (EC3), its Agreements with Third Parties and the Growing Role of Law Enforcement on the European Security Scene, Published in: European Journal of Policing Studies , 2015.
10_ Vittorio Guarriello, Emanuele Macrìe Silvio Marco Guarriello,
Cybercrime: una nuova minaccia per la Pubblica Sicurezza , *Democrazia e Sicurezza Democracy and Security Review, anno XII, n. 1, 2022*.
11_ Olumide Babalola, Nigeria's data protection legal and institutional model: an overview, International Data Privacy Law, Vol. 12, No. 1 , February 2022.

12_ Olumide Babalola, POLICY BRIEF, Data Protection Legal Regime and Data Governance in Africa: An Overview, African Economic Research Consortium, Kenya, No.DG003, February 2022.

13_ Titouche Radia, Territorialité du droit pénal et cybercriminalité , Cahiers de Politique et de Droit , Onzième année – Vol 11 – N° 01 , Janvier 2019 .

4_المواقع الالكترونية باللغة الأجنبية:

1_ Official Council of Europe website: https://www.coe.int

2_Official United Nations website : https://unric.org

3_Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, available at: https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

4_W. Scott Blackmer , Getting Ready for the New EU General Data Protection Regulation, 5 May, 2016, available at: https://web.archive.org/web/20180831164911/https://www.infolawgroup.com/2016/05/articles/gdpr/gdpr-getting-ready-for-the-new-eu-general-data-protection-regulation /

الفهرس

الفهرس:

الملخص:

نظرا لتفاقم الجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، فإن المشرع أضفى حماية جنائية على أنظمة المعالجة الآلية للمعطيات في حالة المساس بالنظام في حد ذاته، أو استهداف العناصر المنطقية المكونة له، أو ارتكاب جرائم باستخدام هذه الأنظمة المعلوماتية.

وتجسدت هذه الحماية الجنائية من خلال خصوصية السياسة الجنائية المتبعة لمكافحة هذه الجرائم على المستوى الدولي حيث تم تعزيز آليات التعاون الدولي التشريعية والإجرائية، والتوجه نحو اعتماد مبدأ الاختصاص الجنائي العالمي بغرض تنسيق هذا التعاون، والخروج عن الأصول الجزائية المتبعة على المستوى الوطني من خلال إقرار أحكام قانونية موضوعية وإجرائية خاصة بهذا النوع من الجرائم.

الكلمات المفتاحية: الأمن السيبراني، الاتفاقيات الدولية، التعاون الدولي، نظام المعالجة الآلية للمعطيات، المعطيات الشخصية.

Résumé:

En raison de l'aggravation des crimes liés aux systèmes de traitement automatisé des données, le législateur a accordé une protection pénale aux systèmes de traitement automatisé des données en cas de violation du système lui-même, de ciblage des éléments logiques qui le composent, ou de commission de crimes en utilisant ces systèmes informatiques.

Cette protection pénale s'est concrétisée à travers la spécificité de la politique criminelle adoptée pour lutter contre ces crimes au niveau international, où les mécanismes de coopération législative et procédurale internationale ont été renforcés de plus, il y a une tendance croissante à adopter le principe de la compétence pénale universelle, qui permet la poursuite de ces crimes, peu importe où ils se produisent, et de sortir des principes pénaux suivis au niveau national en adoptant des dispositions juridiques objectives et procédurales spécifiques à ce type de crimes.

Mots-clés : Cyber sécurité, conventions internationales, coopération internationale, système de traitement automatisé des données, données personnelles.

Abstract:

The rise in crimes targeting automated data processing systems has prompted lawmakers to enact specific legal protections for these systems. These protections cover situations where the system itself is compromised, its internal components are attacked, or crimes are committed using the system.

This new legal framework reflects a shift in criminal justice policy towards combating these crimes on an international scale. This international effort involves strengthening cooperation mechanisms between different countries, both in terms of legislation and procedures. Additionally, there's a growing trend towards adopting the principle of universal criminal jurisdiction, which allows prosecution of these crimes regardless of where they occur. This approach departs from traditional national criminal law and establishes a specialized legal system specifically tailored to address these unique crimes.

Key words: Cyber security, international conventions, international cooperation, automated data processing system, personal data.