

جامعة سعيدة الدكتور مولاي الطاهر



كلية الحقوق والعلوم السياسية  
قسم القانون الخاص

# الحماية القانونية للمعلومات المصنفة والوثائق الالكترونية في البيئة الرقمية

مذكرة لاستكمال متطلبات الحصول على شهادة ماستر في الحقوق  
تخصص: الإدارة الالكترونية

تحت إشراف الأستاذة:  
مولاي ملياني دلال

من إعداد الطلبة:  
كرومي الياس  
صدوقي مصطفى

## أعضاء لجنة المناقشة

|               |             |                            |
|---------------|-------------|----------------------------|
| رئيسا         | جامعة سعيدة | الدكتور بن علي عبد الحميد  |
| مشرفا و مقررا | جامعة سعيدة | الدكتورة مولاي ملياني دلال |
| عضوا          | جامعة سعيدة | الدكتور بن زايد أحمد       |

السنة الجامعية: 2025/2024

## إهداء

نهدي ثمرة هذا الجهد إلى:  
الوالدين الكريمين فخراً واعتزازاً  
جميع أفراد أسرتنا تقديراً واحتراماً  
أساتذتنا وكل من علمنا حرفاً اعترافاً وتبجيلاً  
والى كل من اطلع على هذا العمل  
ودعا لنا بالتوفيق والسداد

## شكر وتقدير

بداية نحمد الله حمداً كثيراً ونشكره على توفيقنا في إتمام هذا العمل المتواضع  
كما نتقدم بأسمى عبارات التقدير والاحترام وخالص شكرنا وعرفاننا  
إلى أستاذتنا طيبة فترة إعدادنا لهذه الدراسة،  
"أ.د. مولاي ملياني دلال"  
لقبولها الإشراف على هذا العمل وعلى كل النصائح والتوجيهات المقدمة.  
فلك منا كل التقدير والامتنان.  
كما نتقدم بأسمى عبارات الشكر والتقدير  
إلى الاساتذة أعضاء لجنة المناقشة  
ولكل أساتذة قسم الحقوق بجامعة سعيدة  
والقائمين عليه على كل المساعدات والمجهودات التي بذلوها معنا  
فلكم منا كل الاحترام.  
كما نتقدم بخالص تشكراتنا إلى كل من ساعدنا في إعداد هذه الدراسة  
من زملاء وأصدقاء

## قائمة المختصرات

| الرمز   | المعنى                              |
|---------|-------------------------------------|
| ج.ر.ج.ج | الجريدة الرسمية للجمهورية الجزائرية |
| دج      | دينار جزائري                        |
| ص       | صفحة                                |
| ط       | طبعة                                |
| م       | ميلادي                              |
| هـ      | هجري                                |

# مقدمة

يشهد العالم اليوم تحولاً جذرياً في طريقة إنتاج المعلومات وتداولها وحفظها، وذلك بفعل التطور الذي يشهده مجال تكنولوجيا المعلومات والاتصالات. وقد أفرز هذا التطور ما يُعرف بـ "البيئة الرقمية" وهي فضاء إلكتروني ديناميكي وتفاعلي يتميز بالانتشار الواسع ولقد أحدثت هذه البيئة تغييرات عميقة في مختلف جوانب حياتنا، بدءاً من طريقة تواصلنا وتبادلنا للمعلومات، وصولاً إلى أساليب عمل المؤسسات وإدارتها لمعلوماتها ووثائقها.

وقد أدى الانتقال إلى البيئة الرقمية إلى بروز أنماط جديدة من الوثائق، مثل الوثائق الإلكترونية، التي لم تعد تعتمد على الدعائم الورقية، بل أصبحت تعتمد على الوسائط الرقمية في إنتاجها وتخزينها وتداولها. وهذا التحول أفرز تحديات قانونية غير مسبوقة، خاصة في مجال حماية المعلومات المصنفة، التي تتطلب درجات عالية من الحماية الإلكترونية.

إن التطور السريع في تكنولوجيا المعلومات والاتصالات، وما يصاحبه من تزايد الهجمات الإلكترونية وسرقة البيانات المصنفة، فرض على الدول ضرورة تحديث تشريعاتها وتكييفها مع هذا الواقع الجديد. ومن هذا المنطلق، بات من الضروري دراسة الإطار القانوني الذي يحكم المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، خاصة في الجزائر التي أصدرت مؤخراً نصوصاً قانونية مهمة في هذا المجال، أبرزها الأمر رقم 09-21 المؤرخ في 8 جوان 2012 المتعلق بحماية المعلومات والوثائق الإدارية، والقانون رقم 04-15 المؤرخ في 1 فيفري 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

هذا البحث يسعى إلى استكشاف الإطار القانوني لحماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، مع التركيز على الآليات القانونية التي تضمن هذه الحماية، وكذا إبراز مدى فعالية المنظومة القانونية الوطنية في مواكبة التهديدات الرقمية الراهنة.

تتمثل الأهمية النظرية لهذا البحث في كونه يساهم في إثراء الإطار المفاهيمي للمعلومات المصنفة والوثائق الإلكترونية في ظل التحول الرقمي، ويعمل على تسليط الضوء على مفهوم البيئة الرقمية كمجال مستحدث يتطلب معالجة قانونية دقيقة ومتكاملة. كما يُبرز البحث العلاقة بين الأمن المعلوماتي وحماية المرفق العام في ظل التحولات الرقمية.

أما من الناحية العلمية، فإن هذه الدراسة تُعد من الدراسات التي تتناول مدى نجاعة الإطار التشريعي الجزائري في مواجهة الجرائم الإلكترونية ذات الصلة بالمعلومات المصنفة والوثائق الإلكترونية، ويُقدم قراءة تحليلية للآليات الوقائية والجزائية ذات الطابع الإلكتروني. وتساهم الدراسة كذلك في فهم مدى تكامل الآليات التقنية والتشريعية والمؤسسية لحماية المعلومات المصنفة و الوثائق الإلكترونية، إضافة إلى دعم جهود البحث العلمي في مجال الرقمنة والإدارة الإلكترونية ضمن العلوم القانونية، خاصة في السياق الجزائري.

وقد جاء اختيار هذا الموضوع بدافع مجموعة من الأسباب، منها ما هو شخصي، مثل التوجه الأكاديمي في تخصص الإدارة الإلكترونية الذي أفرز رغبة ذاتية في اختيار موضوع يندرج ضمن هذا المجال، إلى جانب الاهتمام الشخصي بتطورات البيئة الرقمية وتأثيراتها على القوانين، وارتباط الموضوع بأفاق الباحث الأكاديمية والمهنية.

ومنها ما هو موضوعي، كالتزايد الملحوظ في حالات النشر والإفشاء غير المشروع للوثائق والمعلومات المصنفة، وخاصة بعد اتساع استخدام التكنولوجيات الحديثة داخل الإدارات العمومية، ما يطرح إشكالات أمنية وقانونية. كما يبرز الموضوع الحاجة إلى تقييم فعالية النصوص القانونية المستحدثة ومدى انسجامها مع البيئة الرقمية، خاصة في ظل قصور بعض التشريعات السابقة عن مواكبة التهديدات الإلكترونية الجديدة، خاصة في الجانب الجزائري.

وقد واجهنا خلال هذا البحث بعض الصعوبات، من أهمها ندرة الدراسات الأكاديمية الحديثة في هذا المجال، وحدثة النصوص القانونية، إضافة إلى تداخل الموضوع مع تخصصات علمية أخرى، وحساسية المعلومات المعالجة.

إن التحول الرقمي يشكل تحديًا قانونيًا يستدعي حماية فعّالة للمعلومات المصنفة والوثائق الإلكترونية، ما دفع المشرع الجزائري إلى تحديث تشريعاته لضمان الحماية الفاعلة لها في بيئة رقمية معقدة. ورغم حداثة المنظومة القانونية، تظل فعالية تطبيقها محل تساؤل، خصوصًا في ظل التهديدات الإلكترونية المتزايدة، وضعف جاهزية الإدارات الجزائرية من حيث البنية الرقمية والثقافة القانونية التقنية.

وبناء على ما سبق، يمكن صياغة إشكالية البحث كما يلي:

## هل تكفل المنظومة القانونية آليات فعالة لحماية المعلومات المصنفة والوثائق الإلكترونية في ظل التحديات التقنية التي تفرضها البيئة الرقمية؟

وللإجابة على هذه الإشكالية اعتمدنا على المنهج الوصفي والتحليلي، حيث تم توظيف المنهج الوصفي في ضبط المفاهيم والمصطلحات القانونية المرتبطة بالمعلومات المصنفة والوثائق الإلكترونية، أما المنهج التحليلي فقد استُخدم في دراسة وتفسير النصوص القانونية ذات الصلة، بهدف استخلاص الآليات القانونية المعتمدة لحماية هذه المعلومات والوثائق في ظل البيئة الرقمية.

وللمعالجة هاته الإشكالية المذكورة أعلاه ارتأينا إلى تبني خطة مقسمة إلى فصلين بحث تناولنا في الفصل الأول "الإطار المفاهيمي للمعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية"، وهو بدوره تم تقسيمه إلى مبحثين يتعلقان بمفهوم البيئة الرقمية، وماهية المعلومات المصنفة والوثائق الإلكترونية على التوالي. أما الفصل الثاني الموسوم "بآليات الحماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية"، فتم تقسيمه إلى مبحثين بحيث تم التطرق في المبحث الأول إلى الآليات الوقائية لحماية المعلومات المصنفة والوثائق الإلكترونية وفي المبحث الثاني إلى الآليات الجزائية لحماية المعلومات المصنفة والوثائق الإلكترونية.

# الفصل الأول

الإطار المفاهيمي

للمعلومات المصنفة

والوثائق الإلكترونية في

البيئة الرقمي

يهدف هذا الفصل إلى وضع إطار مفاهيمي واضح ومتكامل للمعلومات المصنفة والوثائق الإلكترونية ضمن سياق البيئة الرقمية. سنسعى إلى استكشاف المفاهيم الأساسية التي تحدد هذه البيئة وخصائصها، بالإضافة إلى التعمق في ماهية المعلومات المصنفة والوثائق الإلكترونية، وأنواعها، وأهميتها، والتحديات المرتبطة بإدارتها في الفضاء الرقمي.

ومنه فقد جرى تقسيم هذا الفصل إلى مبحثين على النحو التالي:

المبحث الأول بعنوان "مفهوم البيئة الرقمية" والذي سنتناول من خلاله التعريف بالمفاهيم الأساسية للبيئة الرقمية، وأهم الخصائص والمكونات التي تميزها. كما سنسلط الضوء على الأسس التي تقوم عليها هذه البيئة وتأثيراتها.

والمبحث الثاني بعنوان "ماهية المعلومات المصنفة والوثائق الإلكترونية" حيث سندرس في هذا المبحث مفهوم الوثائق الإلكترونية وخصائصها وأشكالها المختلفة. بالإضافة إلى تعريف المعلومات المصنفة وأنواعها ومستويات تصنيفها.

من خلال هذين المبحثين، نسعى إلى توفير فهم شامل للإطار المفاهيمي الذي يركز عليه موضوع المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية.

## المبحث الأول: ماهية البيئة الرقمية

يُشكل التحول الرقمي ظاهرة شاملة مست مختلف جوانب الحياة، الإدارية، القانونية، الاقتصادية، والاجتماعية. هذا التحول الذي تقوده تكنولوجيا المعلومات والاتصال، أفرز ما يُعرف بالبيئة الرقمية، وهي الإطار الذي تُنشأ فيه الوثائق الإلكترونية وتُتداول المعلومات المصنفة. وفي سبيل استيعاب هذا التحول، من الضروري التوقف عند مفهوم الرقمنة باعتبارها العملية المؤدية إلى نشوء البيئة الرقمية، واستعراض الأسس التي تقوم عليها هذه البيئة من حيث الخصائص والمتطلبات. وعليه، سيتناول هذا المبحث في مطلبه الأول مفهوم الرقمنة، ثم ينتقل في المطلب الثاني لتحديد ماهية البيئة الرقمية.

### المطلب الأول: مفهوم الرقمنة

تمثل الرقمنة حجر الأساس في الانتقال نحو البيئة الرقمية، فهي عملية تقنية مؤسسية تهدف إلى تحويل الأنشطة والوثائق التقليدية إلى صيغ إلكترونية، ما يفتح المجال أمام تنظيم جديد للعلاقات داخل الإدارات والمؤسسات. وستتم معالجة هذا المطلب عبر ثلاثة فروع: الأول يحدد تعريف الرقمنة، والثاني يبرز الأسباب التي دفعت الدول والمؤسسات إلى تبنيها، أما الفرع الثالث فيعرض الأهداف الأساسية التي تسعى الرقمنة إلى تحقيقها.

### الفرع الأول: تعريف الرقمنة

تنوع المفاهيم المتعلقة بمصطلح الرقمنة وفقاً للإطار أو السياق الذي يستخدم فيه الآلية:<sup>1</sup> بحيث ينظر "تيري كوني Terry Conney"، إلى الرقمنة على أنها عملية تحويل مصادر المعلومات على اختلاف أشكالها مثل: الكتب، والدوريات، والتسجيلات السمعية، والصور الثابتة إلى شكل مقروء بواسطة تقنيات الحاسبات الآلية.

وتشير "شارلوت بورسي Chrriote Pursey" إلى الرقمنة على أنها منهج يهدف إلى تحويل البيانات والمعلومات من النظام التناظري إلى النظام الرقمي.

<sup>1</sup> احمد فرج احمد، الرقمنة داخل مؤسسات المعلومات ام خارجها؟ (دراسة في الاشكاليات ومعايير الاختيار)، مجلة دراسات المعلومات، جامعة الامام محمد بن سعود الإسلامية، السعودية، العدد الرابع، يناير 2009، ص 11.

وتعرف أيضا أنها: "كل عملية يتم عن طريقها تحويل المعلومات من شكلها القديم والتقليدي إلى شكل رقمي سواء كانت هذه المعلومات صور أو بيانات نصية أو ملفات صوتية أو أي شكل آخر".<sup>1</sup>

وتعرف أيضاً أنها: "عملية نقل أي نوع من الوثائق (الورقي) إلى الصنف الرقمي أي عملية تحويل النصوص المكتوبة، المطبوعة أو المخطوطة من صيغتها الورقية إلى صيغتها الرقمية لتصبح قابلة للمعالجة في شاشات الحاسوب".<sup>2</sup>

أيضاً يمكن تعريفها أنها: "عملية استنساخ رقمية تعمل على تحويل الوثيقة أياً كان صنفها إلى سلسلة رقمية مفتوح هذا العمل التقني يسهل فكرياً لتنظيم ما بعد المعلومات من اجل الفهرسة والجدولة وتمثيل محتوى النص المرقمن".<sup>3</sup>

من هذا المنطلق فان الرقمنة حسب ما ورد سابقاً فإنها تأخذ إشكالات عديدة ومتعددة يمكن أن نوجزها فيما يلي:

1. الرقمنة في شكل صورة تشمل الكتب والمخطوطات القديمة خاصة في دراسة القيم الفنية"
2. الرقمنة في شكلها النصي يسمح بالبحث داخل النص مباشرة مع وثائق الالكترونية.
3. الرقمنة في شكل اتجاهي يعتمد على عرض واستبدالها من شكل ورقي إلى شكل العناصر بهدف تبادل ونشر المعلومات المقروءة إلكترونياً.<sup>4</sup>

تماشياً مع هذا فإن مصطلح الرقمنة يأخذ عدة معاني حسب السياق الذي يستخدم فيه إذ يرتبط هذا المفهوم بالإدارة الكترونية حيث يؤكد الكثير من الباحثين على نفس المعنى للمفهومين، فالرقمنة هي استراتيجية إدارية لعصرنة المعلومات والوثائق.

---

<sup>1</sup> عماد عيسى صالح محمد، المكتبات الرقمية الأسس والتطبيقات العلمية، دار المصرية اللبنانية، القاهرة، مصر، ط 1، يناير 2006، ص 219.

<sup>2</sup> زاير نصيرة، عاشور حفيظة، تفعيل الرقمنة في الخدمة العمومية ودورها في تامين الأداء الإداري، مجلة الفكر، جامعة الجزائر 2، المجلد الثامن (العدد الأول)، جوان 2024، ص 400.

<sup>3</sup> نفس المرجع والصفحة سابقا.

<sup>4</sup> نفس المرجع والصفحة سابقا.

## الفرع الثاني: دوافع تطبيق الرقمنة

إن تبني الرقمنة لم يعد خيارًا بل ضرورة لمواكبة هذه التغيرات وتلبية تطلعات المواطنين المتزايدة. ويهدف هذا الفرع إلى التركيز على الدوافع الأساسية لتطبيق الرقمنة يمكن إنجازها في مايلي:

1. تسارع التقدم التكنولوجي والثروة المعرفية المرتبطة به: إن توظيف التكنولوجيا الحديثة لصالح المجتمع وتمكينه من الحصول على فوائد كثيرة يتمثل في تحسين أداء المؤسسات وإتاحة الفرص لها للاستثمار في قطاع التكنولوجيا لتسهيل الحياة والاستفادة من المزايا التقنية المتوفرة على المستوى الدولي.<sup>1</sup>
2. تطوير وتقديم الخدمات الذكية: التركيز على الاستثمار في التكنولوجيا المتقدمة، بما في ذلك الذكاء الاصطناعي وتحليل البيانات، في تصميم وتقديم خدمات رقمية مبتكرة وسهلة الاستخدام. ويهدف إلى تجاوز الخدمات التقليدية من خلال، تلبية احتياجاتهم المتغيرة وتسهيل عليهم الوصول إلى المعلومات وإنجاز المعاملات بكفاءة.
3. رغبة المواطن في تحسين الخدمات: للحصول على خدمات أفضل وأسرع وأسهل في الوصول إلى المعلومات، وقد تدعم هذا الوعي الشعبي بشعور كل مواطن بحقه في الوصول إلى المعلومات ومعرفة آليات اتخاذ القرار السياسي.<sup>2</sup>
4. الكفاءة في تقديم الخدمات العامة: فالكفاءة تأخذ عدة أشكال منها تخفيض الأخطاء، وتحسين الدخل وأيضاً تخفيض التكاليف والتقليل من البيروقراطية من خلال إعادة هندسة الإجراءات، وهذا يؤدي إلى تقليل الوقت المحدد لتحقيق الأهداف وإعطاء الفرصة للموظفين للحصول على مهارات جديدة وتطوير أنفسهم.<sup>3</sup>
5. تحسين العلاقة مع الجمهور: بهدف بناء جسور متينة بين المؤسسات الحكومية والمواطنين، وذلك من خلال تطوير استراتيجيات اتصال فعالة تتسم بالشفافية والاستجابة. ويتضمن ذلك فهمًا عميقًا لاحتياجات وتوقعات الجمهور، واستخدام قنوات متنوعة للتفاعل، مثل المنصات الرقمية ووسائل التواصل الاجتماعي، لتشجيع الحوار والمشاركة الفعالة.

<sup>1</sup> شَارَف صباح، كشرود مروى، دور الرقمنة في عصرة الإدارة الجزائرية (قطاع العدالة نموذجاً)، مذكرة ماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تبسة، الجزائر، 2020/2019، ص 15.

<sup>2</sup> نفس المرجع والصفحة سابقاً

<sup>3</sup> نفس المرجع والصفحة سابقاً

6. حاجة الموظفين الحكوميين للدعم النوعي: من خلال قاعدة معلومات صلبة ونظام عمل متطور وحديث.<sup>1</sup>

7. تمكين الإدارة المحلية: ويتضمن ذلك تعزيز التعاون والتنسيق بين مختلف المستويات الحكومية من خلال المنصات الرقمية، ودعم الحكم الرشيد والمشاركة المجتمعية في صنع القرارات المحلية.

8. تعزيز الشفافية: من خلال إتاحة المعلومات الحكومية للجمهور بسهولة ووضوح، وذلك من خلال استخدام التقنيات الرقمية لتسهيل الوصول إلى المعلومات وتقديمها في صيغ قابلة للاستخدام. ويتضمن ذلك تعزيز ثقافة الشفافية في المؤسسات الحكومية.

9. دفع النمو الاقتصادي الرقمي: من خلال تبيان دور الإدارة الرقمية في تهيئة بيئة مواتية للنمو الاقتصادي، وذلك من خلال تسهيل التجارة الإلكترونية والمعاملات الرقمية، ودعم الابتكار وريادة الأعمال في القطاع الرقمي، وتطوير البنية التحتية الرقمية التي تدعم التنمية المستدامة.

يتضح مما سبق أن تبني الرقمنة لم يعد رفاهية بل ضرورة حتمية تفرضها التطورات المتسارعة وتطلعات الأفراد والمؤسسات. إن الدوافع المتعددة التي تم استعراضها تؤكد على الأهمية القصوى للرقمنة في تحقيق التنمية الشاملة والمستدامة.

### الفرع الثالث: أهداف الرقمنة

تهدف الرقمنة إلى إحداث تحولات إدارية واقتصادية واجتماعية جوهرية في المؤسسات والأفراد وتسعى من خلالها إلى تحسين الكفاءة الداخلية والتفاعل الخارجي، وتحقيق قيمة مضافة للمجتمع وستتناول هذه الأهداف بالتفصيل في هذا الفرع

#### أولاً: الأهداف الإدارية

1. تهدف الرقمنة إلى تحقيق الإدارة بلا ورق، وإدارة بلا مكان، وإدارة بلا زمان، مما يعني توفير المعلومات المتنوعة والمنفتحة التي تتفق مع حاجات الأفراد، وإدارة الوقت بفاعلية لتجاوز الحدود الزمنية والمكانية

2. إدارة الملفات والوثائق بدلا من الحفظ والكتابة

3. استخدام البريد الإلكتروني والمراسلات الإلكترونية بدلاً من الورقية في المعاملات الإدارية

<sup>1</sup> شارف صباح، كشرود مروى، مرجع سابق، ص15.

4. السرية والخصوصية للمعلومات المهمة بحيث تهدف الإدارة إلى امتلاك برامج تمكنها من حجم المعلومات والبيانات المهمة وعدم إتاحتها الا ذوي الصلاحية<sup>1</sup>

#### ثانيا: الأهداف الاقتصادية

1. مساندة برنامج التطوير الاقتصادي وذلك عن طريق تسهيل التعاملات بين القطاع الحكومي والقطاع الخاص وبالتالي زيادة العائد الربحي.<sup>2</sup>
2. إتاحة فرص وظيفية جديدة في مجالات جديدة متعلقة بالرقمنة<sup>3</sup>
3. تشجيع التجارة الإلكترونية والخدمات المالية الرقمية وخلق فرص جديدة للاستثمار الرقمي
4. مراقبة دقيقة للتحصيل الضريبي والجمركي باستخدام أدوات الرقمية وتقليل التهرب الضريبي وزيادة موارد الخزينة العمومية.

#### ثالثا: الأهداف الاجتماعية

1. إيجاد مجتمع معلوماتي قادر على التعامل مع معطيات عصر المعلومات والتكنولوجيا الحديثة.<sup>4</sup>
2. تسهيل التواصل الاجتماعي بين المجتمعات الريفية والمناطق الحضرية عبر وسائل التكنولوجيا الحديثة.
3. تعزيز فعالية الأنظمة الصحية من خلال تكنولوجيا الطب عن بُعد والرقابة الصحية.
4. تمكين الوصول إلى التعليم الرقمي وتوفير محتوى تعليمي متاح عبر الإنترنت.
5. رفع كفاءة الأفراد وتمكينهم من اكتساب المهارات الرقمية التي تؤهلهم لسوق العمل.
6. خدمة المجتمع عبر تطوير رأس المال البشري وتحسين فرص التوظيف.
7. تحسين حياة الأفراد ورفاهيتهم من خلال تطوير الخدمات الاجتماعية الرقمية.<sup>5</sup>

<sup>1</sup> ولد شيخ خولة، بن سعدة سهام، أثر الرقمنة على فعالية الأداء داخل المؤسسة العمومية الجزائرية (دراسة حالة الملحق المحلية لوكالة التشغيل ببلدية شلالة العذارة)، مذكرة ماستر، قسم علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة بجي فارس، المدينة، 2022/2021، ص60

<sup>2</sup> عزيزي عبد السميع، مصطفى وحال، الرقمنة وتحسين الخدمة العمومية في الجزائر، مذكرة ماستر، تخصص دولة ومؤسسات، كلية الحقوق والعلوم السياسية، جامعة بجي فارس، المدينة، 2020/2019، ص22.

<sup>3</sup> نفس المرجع والصفحة سابقا

<sup>4</sup> نفس المرجع والصفحة سابقا

إن الرقمنة بأهدافها الإدارية والاقتصادية والاجتماعية تسعى إلى إحداث نقلة نوعية في أداء المؤسسات وجودة حياة الأفراد. إن تحقيق هذه الأهداف يتطلب تضافر الجهود وتكامل الرؤى للاستفادة القصوى من الإمكانيات التي تتيحها البيئة الرقمية.

### المطلب الثاني: مفهوم البيئة الرقمية

البيئة الرقمية ليست مجرد فضاء إلكتروني، بل هي منظومة متكاملة تتطلب وجود بنية تحتية تكنولوجية وتشريعية وتنظيمية. وللبيئة الرقمية خصوصيات تميزها عن الفضاء المادي، وتفرض شروطاً لضمان فعاليتها وأمنها. بناءً على ذلك، يتناول هذا المطلب تعريف البيئة الرقمية (الفرع الأول)، ثم خصائصها (الفرع الثاني)، وأخيراً المتطلبات الأساسية لقيامها (الفرع الثالث)

### الفرع الأول: تعريف البيئة الرقمية

يمكن تعريف البيئة الرقمية على أنها تلك البيئة التي يجري فيها تناول المعلومات بشكل رقمي من خلال وسائل اتصال جديده تتيح الوصول المباشر والكامل الى المعلومات سواء بشكل تجاري أو خدماتي.<sup>1</sup>

كما تعرف البيئة الرقمية بأنها مجموعة من العناصر متفاوتة المهام والاختصاصات والدرجات الوظيفية والقناعات والكفاءات العلمية المتفاعلة فيما بينها وفق منظومة لإنجاز مهام محددة.<sup>2</sup>

ان البيئة الرقمية قد تداخلت تعريفاتها وتعددت بسبب سرعه تطوراتها من جهة والمهام التي تقوم بأدائها من جهة اخرى ودخولها في مفاصل الحياة اليومية من جهة ثالثة ولا سيما في مجال الوثائق والمعلومات اذ انها تعمل على اتاحة توسيع الادوات والوسائل اللازمة

<sup>5</sup> منجية بورحلة، ساجي الخامسة، منير الحمزة، التحول الرقمي ودوره في تحقيق أهداف التنمية المستدامة، مجلة الدراسات البيئية والتنمية

المستدامة، جامعة الشهيد الشيخ العربي التبسي، الجزائر، المجلد 2، العدد الثاني، 2023، ص126

<sup>1</sup>عبديش عبد الرحيم، بن ناصر محمد، استراتيجيات البحث المتبعة في استرجاع المعلومات في البيئة الرقمية (دراسة ميدانية مع طلبة السنة الثانية ماستر تكنولوجيا وهندسة المعلومات بجامعة عبد الحميد ابن باديس -مستغانم - نموذجاً)، مذكرة ماستر، قسم العلوم الإنسانية، كلية العلوم

الاجتماعية، جامعة عبد الحميد ابن باديس، مستغانم، 2018/2019، ص 43

<sup>2</sup>بوخرياش مولود، ويحة عيسى، تأثير البيئة الرقمية على مكونات الاستراتيجية التسويقية دراسة حالة موقع: Amazon.com، Revue des

Réformes Economiques et Intégration En Economie Mondiale، المدرسة العليا للتجارة، الجزائر، العدد الثاني، 2019، ص3.

لتسهيل الحصول على المعلومات والوثائق وتبادلها وجعلها في متناول مرتديها بسرعه ودقه وفاعليه ليس لها حدود تذكر ولا سيما شبكه الانترنت.

ومما سبق يمكننا القول ان البيئة الرقمية هي الإطار الشامل الذي يجمع بين التقنيات الرقمية المتنوعة كالحواسيب، الإنترنت، الهواتف الذكية، البرمجيات، والمنصات الرقمية وكيفية تفاعل الأفراد والمؤسسات والمجتمعات مع هذه التقنيات وفيما بينها. تتسم هذه البيئة بالديناميكية والتطور المستمر، وتؤثر بشكل عميق على مختلف جوانب الحياة، من التواصل والتعليم والعمل إلى التجارة والترفيه والثقافة.

### الفرع الثاني: خصائص البيئة الرقمية

تميز البيئة الرقمية عن نظيرتها التقليدية بخصائص جوهرية، سنتناول جوانب مثل الحداثة، والترابط الشبكي، والتفاعلية، والافتراضية، لتوضيح كيف تساهم هذه السمات في تشكيل طبيعة التفاعل وتبادل المعلومات في هذا الفضاء.

#### أولاً: الحداثة

حيث أن ما يميز بيئة الإنترنت قدرتها العالية على تجديد معلوماتها، وتعتبر الحداثة صفة ملازمة لمعلومات هذه البيئة التي تتميز بالتجدد السريع للمعلومات، على عكس البيئة التقليدية التي تتصف ببطء شديد في عملية التحديث، وتجديد المعلومات والذي يستغرق وقتاً طويلاً، قد يكون كافياً لتقادم هذه المعلومات في ظل الانتشار الرفيع والتوسع الكبير في إنتاج المعلومات.<sup>1</sup>

#### ثانياً: الترابط والشبكية

تعمل البيئة الرقمية من خلال بنية تحتية من الشبكات والأنظمة المترابطة، حيث تُربط الأجهزة والمستخدمون عبر الإنترنت أو شبكات محلية وعالمية. هذا الترابط يسمح بتبادل المعلومات والبيانات بشكل فوري بين مختلف النقاط، بغض النظر عن المسافات الجغرافية.

<sup>1</sup> زاهي كلثوم، المشاركة المعرفية في ظل البيئة الرقمية (دراسة مسحية على عينة من طلبة السنة الثانية ماستر اتصال وعلاقات عامة مستخدمي صفحة المنبر الإعلامي)، مذكرة ماستر، قسم العلوم الاجتماعية، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، 2019، ص43.

فعندما يرسل شخص بريدًا إلكترونيًا أو يشارك ملفًا عبر منصة الكترونية، تمر هذه البيانات عبر عدة عقد شبكية للوصول إلى الطرف الآخر خلال ثوانٍ. بهذا الشكل، تُمكن الشبكية من بناء منظومة تواصل فعّالة ومستمرة بين الأفراد والمؤسسات حول العالم.

### ثالثًا: التفاعلية

تُبنى التفاعلية في البيئة الرقمية على قدرة الأنظمة والتطبيقات على الاستجابة الفورية لأوامر المستخدمين وتفاعلهم. فعند قيام مستخدم بالنقر على زر، أو إرسال رسالة، أو المشاركة في محادثة مباشرة، فإن النظام الرقمي يعالج هذا التفاعل بسرعة ويُنتج استجابة مناسبة – كفتح صفحة، أو عرض نتيجة، أو بث محتوى. هذه العملية تعتمد على تقنيات مثل البرمجيات التفاعلية، وقواعد البيانات، والذكاء الاصطناعي أحيانًا، والتي تجعل التفاعل بين الإنسان والآلة سلسًا وفوريًا، ما يعزز تجربة المستخدم ويجعل التواصل أكثر حيوية وواقعية.

### رابعًا: الافتراضية

تعتمد البيئة الرقمية على المعلومات التي تُخزّن وتُعالج إلكترونيًا، مما يجعلها غير مادية بطبيعتها. هذا الطابع غير الملموس يسمح بإنشاء فضاءات افتراضية يمكن من خلالها أداء مختلف الأنشطة دون الحاجة إلى وجود مادي فعلي. هذا ما يمنح البيئة الرقمية مرونة عالية، ويجعلها قادرة على تجاوز القيود التقليدية المرتبطة بالمكان والزمن، مما يعزز من كفاءتها وسرعة أدائها.

## الفرع الثالث: متطلبات البيئة الرقمية

البيئة الرقمية، في جوهرها، تتطلب مجموعة من العناصر المتداخلة والمتفاعلة التي تخلق فضاءً يعتمد على التكنولوجيا الرقمية. يمكن تقسيم هذه المكونات الرئيسية إلى ما يلي:

### أولاً: المتطلبات البشرية المؤهلة

تحتاج مشاريع الرقمنة بجوده عالية إلى تكافؤ الكثير من الجهود من مختلف الأشخاص المسؤولين وكلما كان الموظفون مؤهلون يمتلكون مهارات وكفاءات عالية كان ذلك مساعد إذ يعتبر العنصر البشري المغذي للمعلومات والمستقبل لها ورأس المال الحقيقي لأي مشروع.<sup>1</sup>

<sup>1</sup> زاير نصيرة، مرجع سابق، ص401

## ثانيا: المتطلبات التقنية

تُعد المتطلبات التقنية من الأسس الجوهرية لقيام البيئة الرقمية، وتشمل توفير بنية تحتية معلوماتية متطورة تتضمن أجهزة إلكترونية حديثة، وخوادم فعالة، وشبكات اتصال ذات سرعة وأمان عاليين، إلى جانب أدوات الأمن السيبراني الضرورية لحماية البيانات من التهديدات الإلكترونية.

## ثالثا: متطلبات تنظيمية وقانونية

من الناحية التنظيمية والقانونية، فإن البيئة الرقمية تتطلب إطارًا تشريعيًا واضحًا ينظم استخدام التكنولوجيا ويضمن حماية الحقوق والبيانات، مثل قوانين حماية الخصوصية، الجرائم الإلكترونية، وأمن المعلومات والوثائق الإلكترونية. كما يتطلب الأمر وجود سياسات تضبط سلوك المستخدمين.

## رابعا: متطلبات مالية

توافر مستوى مناسب من التمويل المالي بحيث يكون التمويل الحكومي من اجل اجراء الصيانة الدورية وتدريب الكوادر والاداريين والحفاظ على مستوى عالي من تقديم الخدمات ومواكبة أي تطور يحصل في إطار التكنولوجيا.<sup>1</sup>

يتضح لنا مما سبق أن إنشاء بيئة رقمية ناجحة يتطلب تكامل مجموعة من المتطلبات المتنوعة. إن الاستثمار في البنية التحتية التقنية، وتأهيل الكفاءات البشرية، ووضع الأطر التنظيمية والقانونية المناسبة، وتوفير التمويل اللازم، كلها عناصر حاسمة لتعزيز فاعلية وأمان البيئة الرقمية.

## المبحث الثاني: ماهية الوثائق الإلكترونية والمعلومات المصنفة

في ظل التحول الرقمي، ظهرت أنماط جديدة من الوثائق، وأصبحت المعلومات تُصنف وفق معايير دقيقة مرتبطة بسريتها أو حساسيتها. لذلك، يسعى هذا المبحث إلى توضيح ماهية الوثائق الإلكترونية، باعتبارها الوسيلة التي تُحمل عليها المعلومات، ويُعرف بالمعلومات المصنفة

<sup>1</sup> بن نعيم أسماء، دور البيئة الرقمية في تحسين خدمة الإدارة العمومية (دراسة حالة مقرر ولاية المسيلة)، مذكرة ماستر، قسم علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، 2024/2023، ص 17

كموضوع ذي طابع خاص. ويتوزع هذا المبحث على مطلبين: الأول يُعنى بمفهوم الوثائق الإلكترونية، بينما يتناول الثاني المعلومات المصنفة من حيث طبيعتها والمبادئ التي تحكم تصنيفها.

### المطلب الاول: مفهوم الوثائق الإلكترونية

أصبحت الوثائق الإلكترونية من الأدوات الأساسية في الإدارة الرقمية الحديثة، مما يستدعي الإلمام بجميع أساسياتها القانونية والتقنية. في هذا السياق، يتضمن هذا المطلب ثلاثة فروع، حيث يُخصص الأول لتعريف الوثيقة الإلكترونية، بينما يعرض الثاني مكوناتها البنوية، ويختتم الثالث ببيان مزاياها وعيوبها.

### الفرع الاول: تعريف الوثائق الإلكترونية

يُخصص هذا الفرع لعرض مفهوم الوثيقة الإلكترونية من حيث بنيتها الرقمية وطابعها القانوني، وكونها وسيلة لحفظ وإثبات وتداول المعلومات في البيئة الرقمية.

### أولاً: تعريف الوثيقة

جمع وثائق في اللغة، وهو ما يُعتمد به، مؤثت الوثيق (الإحكام في الأمر). نعني بكلمة وثائق جميع وسائل نقل المعرفة وأشكالها المختلفة، مثل: الكتب، الدوريات، الاسطوانات، اللوحات، الأشرطة.<sup>1</sup>

كما يمكن القول أنها آلية ذات مادة ورقية أو آلية إلكترونية تحتوي على بيانات ومعلومات وسجلات استدلالية مصححة سواء على شكل رسالة، تقرير، صورة يعتمد عليها في إثبات الحقائق والدراسات والبحوث والأقوال... الخ مادة تسجيلية من أي نوع مصنوع من الورق تسجل عليها معلومات ووثائقية بصرف النظر عن تكوينها المادي أو خصائصها.<sup>2</sup>

<sup>1</sup> عادل غزال، التسيير الإلكتروني للوثائق، دار للمعية للنشر والتوزيع، قسنطينة، الجزائر، ط 1، 2012، ص13

<sup>2</sup> عبد الغفور عبد الفتاح قارئ، معجم مصطلحات المكتبات والمعلومات: إنجليزي - عربي، الرياض: مكتبة الملك فهد الوطنية، 1420هـ /

## ثانياً: تعريف الوثائق الإلكترونية

الوثائق الإلكترونية هي عبارة عن "معلومات مسجلة ومخزنة على وسيط مادي والتي يمكن تفسيرها في سياق تطبيقي وقد تكون مزيج من نص ورسومات وصورة وصوت أو صور متحركة أو أي أشكال أخرى من المعلومات وقد تتكون من عنصر واحد أو عدة عناصر معا".<sup>1</sup>

ويعرف المشرع الجزائري الوثيقة الإلكترونية بأنها: "مجموعة تتألف من محتوى بينية وسمات العرض تسمح بتهيئتها واستغلالها من قبل الشخص عبر نظام إلكتروني".<sup>2</sup> ويمكن تعريفها بأنها "وثائق تقليدية تم تحويلها إلى شكل رقمي باستخدام المساحات الضوئية، أو تم إنشاؤها باستخدام الحاسوب، والوثيقة الإلكترونية لا تقتصر فقط على الوثائق المخزنة في الأرشيف، كما يعتقد البعض، بل تتعدى ذلك لتشمل مثل الكتب، والدوريات، الصور، خرائط الفيديو ومختلف الوسائط المتعددة".<sup>3</sup>

يتضح مما سبق أن مفهوم الوثيقة الإلكترونية تطور ليشمل أشكالاً متنوعة من المعلومات المسجلة رقمياً، مؤكداً على دورها المحوري من حفظ المعلومات واستعمالها وإثباتها بطرق حديثة، مما يجعل الإمام بها أمراً ضرورياً في ظل العصر الرقمي.

## الفرع الثاني: مكونات الوثيقة الإلكترونية

من خلال هذا الفرع سنقوم بالإلمام بمكوناتها الأساسية للوثيقة الإلكترونية التي تجعل منها وحدة متكاملة صالحة للتداول والاستخدام في البيئة الرقمية. تتمثل العناصر البنائية والتقنية التي تتشكل منها الوثيقة الإلكترونية في ما يلي:

<sup>1</sup> أشرف محمد عبده، إدارة الوثائق الإلكترونية، دار الجوهرة للنشر والتوزيع، القاهرة، 2015، ص28  
<sup>2</sup> المادة 2 الفقرة الأولى من المرسوم التنفيذي رقم 16-142، المؤرخ في 5 ماي 2016، يحدد كفاءات حفظ الوثيقة الموقعة الكترونياً ج.ج.ج.ج، رقم 28، الصادرة في 8 ماي 2016.  
<sup>3</sup> عادل غزال، مرجع سابق، ص14

## 1. المحتوى (Content):

وهو المادة الأساسية التي تتضمنها الوثيقة، مثل النصوص، الصور، الرسومات، الفيديوهات، الجداول، أو أي نوع من البيانات أو المعلومات.

## 2. البنية (Structure):

هذا يتعلق بالبنية المنطقية للوثيقة وتتمثل في الرموز والمعطيات وهي عبارة عن البيانات التي تعرف وتحدد هوية الوثيقة مثل العنوان والجزاء والهوامش والفصول.<sup>1</sup>

## 3. التنسيق (Format):

الصيغة التقنية التي تُحفظ بها الوثيقة مثل: PDF, DOCX, XML، والتي تحدد طريقة عرض وتشغيل الوثيقة على الأنظمة المختلفة.

## 4. الوسيط الإلكتروني:

هو الجهاز أو البيئة التقنية التي تُنشأ أو تُخزن أو تُعرض عليها الوثيقة، مثل الحواسيب، الخوادم، الأقراص الصلبة، أو التخزين السحابي.

## 5. عناصر الأمان:

مثل التوقيع الإلكتروني، التشفير، وكلمات المرور لحماية الوثيقة وضمان مصداقيتها وسلامتها.

## الفرع الثالث: أنواع وأشكال الوثائق الإلكترونية

سوف نتناول في هذا الفرع إبراز أنواع وأشكال الوثائق الإلكترونية، وهو ما يميزها عن الوثائق التقليدية. سنصنف هذه الوثائق بناءً على معايير مختلفة، مثل طريقة إنشائها والشكل الذي تتخذه، لتوضيح مدى مرونتها وقابليتها للتكيف مع مختلف الاحتياجات في البيئة الرقمية.

<sup>1</sup> زيدان فضيلة، حماية وأمن الوثائق الإلكترونية باستخدام تطبيقات الحوسبة السحابية (دراسة على تطبيقات Google Drive وDropbox من وجهة نظر الأساتذة الجامعيين جامعة ابن خلدون تيارت أتمودجاً)، مذكرة مقدمة لنيل شهادة ماستر، قسم علم المكتبات والمعلومات، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة ابن خلدون، تيارت، 2023/2024، ص 15

## أولاً: أنواع الوثائق الإلكترونية

يمكن تقسيم الوثائق الإلكترونية إلى أنواع التالية:

1. الوثيقة ذات المنشأ الإلكتروني: هي الوثيقة التي تُنشأ إلكترونياً بواسطة الحاسوب في مختلف الأشكال (DOC, XML, XLS, HTML, ...). وتتم معالجتها إلكترونياً.
2. الوثيقة المرقمنة: هي الوثائق التي تم تحويلها من شكلها الورقي إلى شكل رقمي باستخدام تقنيات المسح الضوئي.
3. الوثيقة الهجينة: هي الوثائق التي تمزج بين النوعين السابقين، قد تكون وثيقة نصية منشأة باستخدام الحاسب الآلي وإضافة صورة تمت رقمتها مثلاً: تقوم بكتابة سيرتك الذاتية باستخدام معالج النصوص، ثم تقوم برقمنة صورتك الشخصية أي تحويلها إلى شكل ملف إلكتروني ليتم دمج مع الملف النصي المنشأ وينتج عنه وثيقة مختلطة.

يمكن القول هنا أن الاختلاف يكون فقط في الإنشاء، سواء كانت الوثيقة ذات منشأ تقليدي تمت رقمتها أو منشأ إلكتروني، لكن في نفس الوقت يمكن مزج النوعين السابقين في وثيقة واحدة إلكترونية، وفي الأخير يتضح كل ما سبق جمعه أو تحويله أو إنشائه وثيقة إلكترونية يتم التعامل معها في البيئة الرقمية، وذلك بطبيعة الحال لتشمل المحتوى المعلوماتي الرقمي.<sup>1</sup>

## ثانياً: أشكال الوثيقة الإلكترونية

تتمتع الوثيقة الإلكترونية بأشكال مختلفة، وهي كالتالي:

1. الوثائق النصية: هي الوثائق التي يتم إنشاؤها من خلال مجموعة من البرامج التي تكون على سطح المكتب مثل برامج معالج النصوص \*Office\* مثل برنامج \*Word\* و \*Excel\*، وهي عبارة عن نصوص ووثائق العروض التقديمية ووثائق الجداول الحسابية.

<sup>1</sup> زيدان فضيلة، مرجع سابق، ص 16

2. وثائق الوسائط المتعددة: هي الوثائق التي يتم إنشاؤها بمختلف الوسائط فتكون متنوعة ومزج بين النص والصورة المتحركة أو الثابتة أو الصوت مثل الوثائق السمعية المرئية ورسائل البريد الإلكتروني.

3. وثائق متعددة الأبعاد: هي الوثائق التي يتم إنشاؤها بواسطة استخدام نظم معلومات إدارية مثل قواعد البيانات، نظم (إرضاء العملاء، نظم إدارة المحتوى، نظم الموارد البشرية).<sup>1</sup>

### الفرع الرابع: مميزات وسلبيات الوثيقة الإلكترونية

على الرغم من الانتشار الواسع لاستخدام الوثائق الإلكترونية لما توفره من مرونة وكفاءة، إلا أن اعتمادها يطرح تحديات متعددة تتعلق بالأمان، والبنية التحتية، والملائمة التكنولوجية. في هذا الفرع، نستعرض مزايا الوثائق الإلكترونية، إلى جانب أبرز عيوبها التي تتطلب حلولاً تقنية وتنظيمية.

### أولاً: مميزات الوثيقة الإلكترونية

تتميز الوثيقة الإلكترونية بعدة مميزات أهمها:<sup>2</sup>

1. حركية: أي أنها تحتوي على نص وصوت وصورة متحركة أو ثابتة في نفس الوقت ومتنوعة

الأصول ويمكن أن تظهر في عدة مكونات مثل: (HTML – DOC – MP3 – SJPEJ – PDF – XL)

2. المرونة وقابلية التغيير: تتميز الوثائق الإلكترونية بالمرونة وقابلية التعديل والتغيير في مضمون الوثيقة الإلكترونية أو شكلها أو تنسيقها.

3. الذاتية: الاستعمال الذي للوثائق الإلكترونية بإمكان المستخدم الوصول والاطلاع على الوثيقة الرقمية من أي جهاز سواء كان هاتف ذكي أو جهاز حاسوب بمختلف أنظمة التشغيل.

<sup>1</sup> عادل غزال، مرجع سابق، ص15

<sup>2</sup> زيدان فضيلة، مرجع سابق، ص21

4. الصيغة الحيوية والديناميكية للوثيقة الإلكترونية: إمكانية النقل والتصفح بكل حرية عبر الأجهزة من خلال تقنية النص الفائق والنص التشعبي.

ثانيا: سلبات الوثائق الإلكترونية:

1. الوثائق الإلكترونية غير مادية، وهي تحتاج إلى وسط كالحاسوب من أجل قراءتها من طرف المستفيد، خاصة مع ظهور المعلومات الافتراضية الموجودة على الشبكات المعلوماتية.
2. إمكانية تعرض الوثائق الإلكترونية للسرقة والتلاعب والتحريف.
3. التطور السريع لبرامج الأجهزة ووسائل التخزين والتي قد لا يمكن ملاءمتها، مما يؤكد على ضرورة إيجاد سياسة واضحة للإدارة وتوفير وسائل وأجهزة لاسترجاع الوثائق الإلكترونية.
4. يتطلب الاعتماد على الوثائق الإلكترونية بنية تحتية تكنولوجيا كبيرة واختصاص في إعداد الملفات وتطويرها ومتابعتها من حين إلى آخر لتحديثها.
5. تعرض أجهزة الكمبيوتر التي حازت ملفات الأعمال والمستندات الكبيرة إلى فيروسات تؤثر على البيانات المحفوظة.<sup>1</sup>

ويتضح لنا مما سبق أن الوثيقة الإلكترونية تُعد خياراً إستراتيجياً في الإدارة الرقمية المعاصرة، لما توفره من مزايا عديدة على مستوى السرعة والفعالية والتخزين. ومع ذلك، تبقى الحاجة قائمة لتجاوز عيوبها من خلال تطوير الأطر التقنية والتنظيمية التي تضمن سلامتها وسهولة استخدامها بشكل مستدام.

### المطلب الثاني: مفهوم المعلومات المصنفة

تكتسي المعلومات المصنفة أهمية خاصة في البيئة الرقمية، نظراً لما تحتويه من معطيات تمس الأمن العام أو المصالح الاستراتيجية. وتُضبط هذه المعلومات وفق معايير قانونية دقيقة تحدد طبيعتها ودرجات تصنيفها. ويُعالج هذا المطلب من خلال أربعة فروع رئيسية: الأول لتعريف

<sup>1</sup> كحيلة سارة، إدارة الوثائق الإلكترونية (دراسة تقييمية لمشروع وزارة التربية الوطنية)، أطروحة مقدمة لنيل شهادة دكتوراه طور الثالث ل.م.د في علم المكتبات والتوثيق، قسم علم المكتبات والتوثيق، كلية العلوم الإنسانية، جامعة الجزائر 2، الجزائر، 2021/2020، ص41

المعلومات، الثاني لبيان خصائصها وطبيعتها القانونية، الثالث لعرض المبادئ المنظمة لتصنيفها، والرابع لتحديد مستويات التصنيف المعتمدة.

### الفرع الأول: تعريف المعلومات المصنفة

يعرض هذا الفرع تعريف المعلومات المصنفة باعتبارها كل محتوى أو مضمون معرفي يُستعمل لأغراض تنظيمية أو قانونية، ويُعد موضوعاً للحماية القانونية.

#### أولاً: تعريف المعلومات

المعلومات من حيث مدلولها اللغوي مشتقة من المادة اللغوية (علم)، وهي مادة غنية بالكثير من المعاني كالعالم والإحاطة ببواطن الأمور والوعي والإدراك، واليقين، والإرشاد، والإعلام، والشهرة، والتميز، والتحديد للمعالم، والمعرفة، والتعليم، والتعلم، والدراية... إلى آخر ذلك من المعاني المتصلة بوظائف العقل.<sup>1</sup>

أما اصطلاحاً هي البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد، لأغراض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، أو تفسيرها، أو تنظيمها في شكل ذي معنى وإلى وإلى يمكن تداولها وتخزينها ونشرها وتوزيعها في صورة رسمية أو غير رسمية وهي أي شكل.<sup>2</sup>

كما عرفت المعلومات في قاموس البنهاوي الموسوعي على أنها: "الحقائق الموصلة" ولها تعريف آخر بأنها "رسالة تستخدم لتمثيل حقيقة أو مفهوم باستخدام وحدة وسط بيانات"، كما عرفت بأنها عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة".<sup>3</sup>

<sup>1</sup>رشدي محمد علي، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الأنترنت، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ط 1، 2000، ص 45

<sup>2</sup>أحمد محمد الشامي سيد حسب الله، المعجم الموسوعي لمصطلحات المكتبات والمعلومات (انجليزي-عربي)، دار المريخ للنشر، السعودية، ط 1، 1988، ص 980

<sup>3</sup>د.شعبان خليفة، قاموس البنهاوي الموسوعي(عربي)، العربي للنشر والتوزيع، الرياض، السعودية، ط 1، 1990، ص 400

ومن الجانب القانوني فبالرجوع إلى الأمر 09-21 المتعلق بحماية المعلومات والوثائق الادارية فقد عرف لنا المشرع الجزائري المعلومات بأنها: "أي حدث أو خبر مهما كان مصدره وثيقة أو صورة أو شريط صوتي أو مرئي أو سمعي بصري أو محادثة أو مكالمة هاتفية يؤدي الكشف عنها الى المساس بالسلطات المعنية".<sup>1</sup>

### ثانيا: تعريف المعلومات المصنفة

هي كل مكتوب ورقي أو الكتروني أو رسم أو مخطط أو خريطة أو شريط صوتي أو سمعي بصري أو أي سند مادي أو الكتروني آخر كانت محل تدابير ترمي إلى منع نشرها أو تقييد الاطلاع عليها.<sup>2</sup>

كما تعتبر المعلومات المستقاة اثناء عمليات المراقبة او التفتيش من طرف الجهات المختصة في إطار التحقيقات القضائية عبارة عن معلومات مصنفة.<sup>3</sup>

### الفرع الثاني: الخصائص والطبيعة القانونية للمعلومات

تكتسي المعلومات أهمية بالغة، إذ تستمد أهميتها من طبيعتها الخاصة ومن الخصائص التي تجعل منها موضوعاً للحماية القانونية. ومن أجل ضبط هذا المفهوم، كان لا بد من تحديد السمات التي تتوافر في المعلومة حتى تكتسب هذه الحماية.

### أولاً: خصائص المعلومات

لستفيد المعلومة بالحماية القانونية لا بد أن تتوافر فيها مجموعة من الخصائص تتجلى فيما يلي:<sup>4</sup>

#### 1. خاصية التحديد:

يجب أن تكون المعلومة محددة، فإذا عدم تحديدها تكون المعلومة منعدمة، فالمعلومة المحددة هي التي تكون محصورة في إطار معين.

<sup>1</sup>أنظر المادة 02 من الامر 09-21 المتعلق بحماية للمعلومات والوثائق الإدارية، المؤرخ في 9 يونيو 2021، ج.ر.ج.ج، العدد 45، المؤرخة في 9 يونيو 2021.

<sup>2</sup> المادة 3 فقرة 3، الامر 09-21، مرجع سابق

<sup>3</sup> المادة 24 من المرسوم الرئاسي 20-183، مرجع سابق.

<sup>4</sup> مريم ثابت، مرجع سابق، ص 11

## 2. خاصية الابتكار:

يجب أن تكون المعلومة مبتكرة أي تتسم بالأصالة ولم تكن موجودة من قبل. وبمفهوم المخالفة، فإن المعلومة غير المبتكرة لا تعد معلومة بالمفهوم الفني الدقيق لهذه الكلمة، فهي لا ترتبط بشخص معين وليست ملك أحد.

## 3. خاصية السرية:

يقصد بها أن تكون المعلومة محاطة بحدار من السرية، أي ضرورة الاحتفاظ بهذه المعلومة في نطاق محدد من الأشخاص، أي أن تكون الرسالة التي تحملها محددة بمجموعة من الأشخاص. وبدون هذه السرية فالمعلومة تكون شائعة بين الناس وبالتالي لا تتمتع بأي حماية جزائية، فصفة السرية لازمة في المعلومة.

## 4. خاصية الاستثارة:

تعتبر خاصية الاستثارة بالمعلومة أمرًا هامًا في جميع الجرائم التي تتطور على الاعتداء القانوني القائم، حيث يستأثر الفاعل بسلطة تخص الغير وعلى نحوٍ مطلق. وتتوفر المعلومة على صفة الاستثارة إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين.

## ثانيا: الطبيعة القانونية للمعلومات

إن الطبيعة القانونية للمعلومات تعد أساس الحماية القانونية المقررة لها، وانقسم الفقه في تحديد طبيعتها القانونية إلى اتجاهين:

## 1. الاتجاه التقليدي:

يرى أصحاب هذا الاتجاه أن المعلومات لها طبيعة من نوع خاص، فهي -وفقًا لهم- ذات طبيعة معنوية وليست ذات طبيعة مادية، فهي مرتبطة بالخدمة أو المنفعة، ويعاب على هذا الاتجاه إهمال القيمة المالية للمعلومة، وأيضًا الخلط بينها وبين الخدمة أو المنفعة التي يمكن تقويمها بالمال، ونتجت عن ذلك صعوبة تقرير الحماية القانونية للمعلومات.<sup>1</sup>

<sup>1</sup> عبد الرحمن بوكفة، الحماية القانونية للمعلومات والوثائق الإدارية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص القانون العام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، 2023/2022، ص12

## 2. الاتجاه الحديث:

يرى أنصار هذا الاتجاه أن المعلومات مجموعة من القيم، فهي ذات طبيعة مادية، نظرًا للقيمة الاقتصادية للمعلومة، التي ترتبط بصاحبها، ما يضمن سريتها وقيام المسؤولية عن أي عمل غير مشروع يتعلق بها.<sup>1</sup>

### الفرع الثالث: المبادئ الرئيسية لتصنيف المعلومات

تستند عملية تصنيف المعلومات إلى مجموعة من المبادئ التنظيمية التي تهدف إلى تحقيق التوازن بين حق الإتاحة ومتطلبات السرية، وتأتي هذه المبادئ استجابة لتطور البيئة الرقمية يمكننا إيجازها في ما يلي:

#### المبدأ الأول: الأصل في المعلومات الإتاحة

الأصل في المعلومات أن تكون متاحة ما لم تقتض طبيعتها أو حساسيتها مستويات أعلى من التصنيف والحماية.

#### المبدأ الثاني: الضرورة والتناسب

يتم تصنيف المعلومات إلى مستويات وفقاً لطبيعتها، ومستوى حساسيتها، ودرجة أثرها مع الأخذ بعين الاعتبار الموازنة بين قيمتها ودرجة سريتها

#### المبدأ الثالث: التصنيف في الوقت المناسب

يتم تصنيف المعلومات عند إنشائها أو حين تلقيها من جهات أخرى ويكون التصنيف خلال فترة زمنية محددة.

#### المبدأ الرابع: المستوى الأعلى من الحماية

يتم اعتماد المستوى الأعلى من التصنيف عندما يتضمن محتوى متكاملًا من البيانات مستويات تصنيف مختلفة.

<sup>1</sup> نفس المرجع، ص 13

## المبدأ الخامس: فصل المهام

يتم الفصل بين مهام ومسؤوليات الموظفين، فيما يتعلق بتصنيف المعلومات أو الوصول إليها أو الإفصاح عنها أو استخدامها أو التعديل عليها أو إتلافها، بطريقة تحول دون تداخل الاختصاص والصلاحيات.

## المبدأ السادس: الحاجة إلى المعرفة

يتم تقييد الوصول إلى المعلومات واستخدامها على أساس الاحتياج الفعلي للمعرفة، وأقل عدد ممكن من العاملين.

## المبدأ السابع: الحد الأدنى من الامتيازات

يتم تقييد إدارة صلاحيات الموظفين على الحد الأدنى من الامتيازات اللازمة لأداء المهام والمسؤوليات المناطة بهم.<sup>1</sup>

إنّ المبادئ الرئيسية لتصنيف المعلومات لا تكفي بتحديد ضوابط تنظيمية لحماية البيانات، بل تمثل الإطار الهيكلي الذي تُبنى عليه حوكمة المعلومات داخل المؤسسات والإدارات العمومية، سواء في البيئة التقليدية أو الرقمية.

وتقوم هذه المبادئ - مثل "الضرورة والتناسب" و"الحاجة إلى المعرفة" و"فصل المهام" على إيجاد توازن دقيق بين الحق في المعرفة والحق في السرية، فكلما كانت المعلومات أكثر حساسية، كانت الحاجة إلى تنظيم تداولها وحصر الوصول إليها ضمن نطاق ضيق، لضمان عدم استغلالها أو تسريبها بما يضر بالمصلحة العامة

## الفرع الرابع: مستويات تصنيف المعلومات

صنف المشرع الجزائري المعلومات على أساس درجة حساسيتها بموجب نص المادة السادسة من الأمر 09-21 المتعلق بحماية المعلومات والوثائق الإدارية إلى ما يلي:

<sup>1</sup> سياسة تصنيف البيانات، مكتب إدارة البيانات، هيئة حقوق الانسان السعودية، الاصدار الأول، 2021، ص 10

### 1. معلومات ووثائق سرية جداً:

الوثائق السرية جداً هي تلك الوثائق التي يترتب على إفشائها المساس بالأمن الوطني في الداخل والخارج أو بمصالح الدولة.

### 2. معلومات ووثائق سرية:

وتتضمن الوثائق السرية الوثائق التي يلحق إفشاؤها ضرراً خطيراً بمصالح الدولة.

### 3. معلومات ووثائق واجبة الكتمان:

وتكون الوثائق واجبة الكتمان تلك الوثائق الأقل خطورة وحساسية، إلا أن إفشاؤها قد يتسبب بأضرار مؤكدة لمصالح الحكومة أو الإدارات المركزية أو اللامركزية سواء كانت محلية أو مرفقية أو إحدى الهيئات العمومية، ويترتب على إفشائها متابعة الموظف تأديبياً ومدنياً وجزائياً.

### 4. معلومات ووثائق محدودة التوزيع:

الوثائق محدودة التوزيع هي تلك الوثائق التي لا يمكن لأي كان الاطلاع عليها بل فقط من يملكون المكانة القانونية لذلك، أو حوّلتهم مصالح الدولة صراحة الاطلاع عليها بحكم وظيفتهم أو المهمة الموكلة إليهم.<sup>1</sup>

ومما سبق يتضح لنا أن تصنيف المعلومات إلى سرية جداً، وسرية، وواجبة الكتمان، ومحدودة التوزيع، يعكس رؤية تشريعية منهجية تهدف إلى حماية المصالح العليا للدولة، ويضبط نطاق الاطلاع والاستخدام بناءً على معايير مدروسة. كما أن هذا التصنيف يُعدّ أداة عملية لتحقيق الحماية القانونية للمعلومة في ظل التحولات الرقمية المتسارعة، ويؤكد أهمية السرية كشرط أساسي لتفعيل هذه الحماية.

<sup>1</sup> أنظر المادة 06 من الامر 09-21، مرجع سابق.

ختامًا، يمكن القول إن هذا الفصل قد شكّل الأساس النظري للدراسة، من خلال ضبط المفاهيم المحورية المرتبطة بالوثائق الإلكترونية والمعلومات المصنفة والتركيز على تبيان السياق العام الذي تنشأ فيه هذه الوثائق والمعلومات، في ظل التحول الرقمي الواسع الذي يشهده العالم، بما يفرضه من متطلبات جديدة على مستوى حفظ المعلومات، تداولها، وحمايتها.

ويُعد هذا التمهيد النظري خطوة أساسية لفهم أعمق للإشكالات القانونية التي تثيرها عملية حماية المعلومات المصنفة والوثائق الإلكترونية، خصوصًا في ظل ما أفرزته التطورات التقنية المتسارعة من تحديات غير مسبقة، سواء على مستوى التشريع أو الممارسة العملية.

وفي ضوء ذلك، سيُخصص الفصل الثاني من هذه الدراسة لبحث النصوص التي أقرها المشرّع الجزائري إلى جانب بعض الآليات التقنية والمؤسسية بهدف ضمان حماية فعالة لهذه الفئة من الوثائق والمعلومات. وسيتم التطرق في هذا الإطار إلى التدابير ذات الطابع الوقائي، وكذا تلك ذات الطبيعة الجزائية، بالنظر إلى أهمية التوازن بين المنع والعقاب في تحقيق الأمن المعلوماتي ضمن البيئة الرقمية.

# الفصل الثاني

آليات حماية المعلومات

المصنفة والوثائق

الالكترونية في البيئة

الرقمية

في ظل التحول الرقمي الذي يشهده العالم، أضحت المعلومات المصنفة والوثائق الإلكترونية تمثل ركيزة أساسية في عمل الإدارات والمؤسسات، نظراً لما تحتويه من بيانات حساسة تمس الأمن الوطني والنظام العام. إلا أن هذا الانتقال إلى البيئة الرقمية رافقته مخاطر متزايدة تهدد سرية وسلامة هذه المعلومات، مما أفرز ضرورة ملحة لوضع إطار قانوني فعال يؤمن حمايتها ويحد من التهديدات المرتبطة بها.

ومن هذا المنطلق، برز دور المشرع في سنّ مجموعة من الآليات القانونية لضمان حماية هذه المعلومات، تتنوع بين إجراءات وقائية تهدف إلى تعزيز الأمن المعلوماتي والرقابة التقنية والمؤسسية، وآليات ردعية تهدف إلى معاقبة كل من تسوّل له نفسه اختراق أو نشر أو استغلال هذه البيانات بطرق غير مشروعة.

وبناءً على ما سبق، سيُخصص هذا الفصل لتسليط الضوء على هذه الآليات القانونية، من خلال التطرق في المبحث الأول إلى الآليات الوقائية المعتمدة لحماية المعلومات المصنفة والوثائق الإلكترونية، في حين يُعالج المبحث الثاني الجانب المتعلق بـ الآليات الجزائية، مُبرزاً صور الجرائم المرتكبة في هذا السياق والعقوبات المقررة لها.

## المبحث الأول: الآليات الوقائية لحماية المعلومات المصنفة والوثائق الالكترونية

نتقل في هذا المبحث الأول إلى استكشاف الآليات الوقائية التي تهدف إلى حماية هذه الأصول الرقمية الحساسة قبل وقوع أي تهديد أو انتهاك. فالحماية الاستباقية تعتبر خط الدفاع الأول في مواجهة المخاطر المتزايدة في الفضاء الرقمي.

سنتناول في هذا المبحث ثلاثة مطالب أساسيين يمثلون ركيزتي الحماية الوقائية: الحماية التشريعية التي توفر الإطار القانوني المنظم لهذه الحماية والآليات التقنية الداعمة للإطار القانوني والحماية المؤسساتية التي تقدم الأدوات والوسائل العملية لتطبيق وتنفيذ هذه الحماية في البيئة الرقمية.

### المطلب الأول: الحماية التشريعية

في هذا المطلب الأول، سنتناول بالتفصيل الحماية التشريعية المقررة في الجزائر لهذا النوع من المعلومات والوثائق. وسنركز بشكل خاص على تحليل واستعراض أهم الأحكام الواردة في الأمر رقم 09.21 المتعلق بحماية المعلومات والوثائق الإدارية،<sup>1</sup> والقانون رقم 04.15 المتعلق بالتوقيع والتصديق الإلكترونيين.<sup>2</sup> سنسعى إلى فهم كيف ينظم هذان النصان القانونيان حماية المعلومات المصنفة والوثائق الإلكترونية، وما هي الالتزامات التي يفرضانها، والحقوق التي يقرانها في هذا السياق.

### الفرع الأول: الأمر رقم 09-21 المتعلق بحماية المعلومات والوثائق الإدارية

يُعد الأمر رقم 09-21 الإطار القانوني الأهم في التشريع الجزائري فيما يتعلق بحماية المعلومات والوثائق الإدارية، لا سيما المصنفة منها. وبالخصوص في ظل التحولات الرقمية التي تعرفها الإدارة العمومية. وعليه سوف نتناول في هذا الفرع تعريف بالأمر 09-21 ودوافع صدوره وسياقه وكذا دوره في حماية المعلومات والوثائق.

### أولا: تعريف بالأمر رقم 09-21 المتعلق بحماية المعلومات والوثائق الإدارية

الأمر رقم 09-21 المؤرخ في 8 جوان 2021، يُعد بمثابة الإطار القانوني المرجعي الذي وضعت الجزائر لتأطير مسألة حماية الوثائق الإدارية والمعلومات المصنفة.

<sup>1</sup> الأمر 09-21، مرجع سابق.

<sup>2</sup> القانون رقم 04-15، المؤرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ح.ر.ج.ج، العدد 06، الصادرة بتاريخ 20 ربيع الثاني عام 1436 هـ الموافق 10 فبراير سنة 2015.

لقد أشارت المادة الأولى إلى أن الهدف من هذا الأمر هو حماية المعلومات والوثائق الإدارية للسلطات العمومية. وبمنظرة أولية حول أهم أحكامه، نجد أنه يتضمن 51 مادة موزعة على 07 فصول. تناول المشرع من خلالها مختلف القواعد القانونية التي تهدف إلى تأمين سرية المعلومات والوثائق الإدارية للسلطات العمومية. فقد تناول الفصل الأول، المعنون بـ "أحكام عامة"، مجموعة من المفاهيم والمصطلحات متعددة الصلة بهذا الأمر. كما عالجت الفصول المتبقية مختلف الأحكام التنظيمية والإدارية الرامية إلى تأمين وحماية المعلومات والوثائق، لاسيما المصنفة منها. وأخيراً، تم تناول مسألة التجريم والعقاب في حال المساس بسلامة محتويات هذه الوثائق. إن المعالجة التشريعية المستشفة من خلال أحكام هذا القانون تبين استخدام مختلف الوسائل الرامية إلى تأمين سرية المعلومات والوثائق الإدارية. وقد اقتضت هذه المعالجة عدة آليات تم تجسيدها من خلال مختلف نصوص هذا القانون.<sup>1</sup>

وقد جاء هذا الأمر لسد فراغ قانوني كان واضحاً في مجال أمن الوثائق والمعلومات الالكترونية ذات الطابع الحساس داخل المؤسسات العمومية، خاصة مع تزايد التهديدات السيبرانية وتوسع استعمال الوسائط الرقمية في الإدارة.

### ثانياً: دوافع صدور الأمر 09-21 وسياقه

صدر الأمر 09-21 في سياق يتسم بارتفاع حجم التحديات التي تواجهها المؤسسات العمومية في ظل التحول الرقمي المتسارع، وما يرافقه من أخطار حقيقية تتعلق باختراق الأنظمة وسرقة أو تسريب المعلومات. وبالنظر إلى أن الوثائق الإدارية قد تحتوي على بيانات تتعلق بالأمن الوطني، أو بمصالح استراتيجية للدولة، كان من الضروري وضع إطار قانوني يُعنى صراحة بحمايتها كما يعكس هذا النص إرادة الدولة الجزائرية في تعزيز سيادتها المعلوماتية، عبر آليات قانونية وتقنية حديثة، تُضفي على الوثيقة الإلكترونية نفس القدر من الحماية الممنوح للوثيقة الورقية، بل أكثر في بعض الجوانب، بالنظر لطبيعة التهديدات الرقمية.

### ثالثاً: دور الأمر 09-21 في حماية المعلومات والوثائق المصنفة

بناءً على الأمر رقم 09-21 المؤرخ في 8 جوان 2012، المتعلق بحماية المعلومات والوثائق الإدارية، يمكن تلخيص دوره في حماية المعلومات المصنفة والوثائق الإلكترونية في النقاط التالية:

<sup>1</sup> محمد بن فريدة، "آليات حماية المعلومات والوثائق الإدارية - دراسة من خلال أحكام الأمر 09-21"، المجلة الدولية للبحوث القانونية والسياسية، العدد 03، ديسمبر 2021، ص118

1. التصنيف حسب درجة الحساسية: يصنف الأمر الوثائق إلى أربع فئات (سري جداً، سري، واجب الكتمان، توزيع محدود) حسب درجة الحساسية وتأثير إفشائها على الأمن الوطني أو المصلحة العامة بحيث يمثل ذلك خطوة استباقية حاسمة لتحديد مستويات الحماية.<sup>1</sup>
  2. الإلزام بالحماية والسرية: يُلزم السلطات العمومية باتخاذ تدابير أمنية وتقنية لحماية الوثائق والمعلومات المصنفة من التسريب أو الاطلاع غير المصرح به أو التوزيع غير القانوني.<sup>2</sup>
  3. ضمان التكوين والتأهيل: يشترط الأمر أن يخضع الموظفون المعنيون بتداول الوثائق المصنفة لتكوين خاص يمكنهم من التعامل الآمن مع هذه الوثائق.<sup>3</sup>
  4. منع التوزيع غير المصرح به: يمنع توزيع أو نشر أو حتى الاطلاع على الوثائق المصنفة إلا من قبل الأشخاص المؤهلين وبترخيص مسبق.<sup>4</sup>
  5. تحديد المسؤوليات: يحتمل الأمر الأشخاص الذين يتسببون في إفشاء أو تسريب الوثائق المصنفة مسؤولية قانونية، سواء كانت مدنية، تأديبية أو جزائية.<sup>5</sup>
  6. حماية ومصادقية للوثائق الإلكترونية: يشمل الحماية أيضاً الوثائق الإلكترونية باعتبارها وثائق رسمية، ويمنع قرصنتها أو نسخها أو تداولها بطرق إلكترونية دون إذن.<sup>6</sup>
  7. العقوبات الصارمة: ينص الأمر على عقوبات تصل إلى السجن والغرامة ضد كل من يثبت ضلوعه في نشر أو إفشاء أو تسريب وثائق مصنفة، سواء عن قصد أو نتيجة إهمال.<sup>7</sup>
- الفرع الثاني: القانون رقم 04-15 الذي يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكتروني

يشكل القانون رقم 04-15 خطوة محورية في سبيل تعزيز الثقة القانونية في الوثائق الإلكترونية من خلال تنظيم التوقيع والتصديق الإلكترونيين. ويأتي هذا القانون في سياق التوسع المتزايد في المعاملات الرقمية، وضرورة ضبطها بإطار قانوني يضمن سلامتها ومصداقيتها. وعليه،

<sup>1</sup> المادة 6 من الامر 09-21، مرجع سابق

<sup>2</sup> المادة 7 من الامر 09\_21، نفس المرجع

<sup>3</sup> المادة 7 الفقرة الأخيرة من الأمر 09\_21، نفس المرجع

<sup>4</sup> المادة 8 من الامر 09\_21، نفس المرجع

<sup>5</sup> المادة 21 من الامر 09\_21، نفس المرجع

<sup>6</sup> المادة 3 الفقرة 3 من الامر 09\_21، نفس المرجع

<sup>7</sup> المادة 28 الى 43 من الامر 09\_21، نفس المرجع

سنتطرق في هذا الفرع إلى التعريف بالقانون 04-15، دوافع صدوره وسياقه، بالإضافة إلى دوره في حماية الوثائق الإلكترونية.

**أولاً: تعريف بالقانون رقم 04-15 الذي يحدد القواعد المتعلقة بالتوقيع والتصديق الإلكتروني.**

يُعد القانون رقم 04-15 المؤرخ في 1 فيفري 2015 أول إطار تشريعي جزائري متكامل يُعنى بتنظيم مسألة التوقيع والتصديق الإلكترونيين. وقد جاء هذا النص القانوني ليُجسد التوجه الرسمي نحو إدماج تكنولوجيا المعلومات والاتصال ضمن آليات التسيير الإداري والاقتصادي، حيث يهدف إلى إضفاء الشرعية القانونية على الوثائق الإلكترونية من خلال الاعتراف بالتوقيع الإلكتروني كوسيلة فعالة لإثبات المعاملات الإلكترونية، تماماً كما هو الحال بالنسبة للتوقيع الخطي في الوثائق الورقية.

ويضم هذا القانون 82 مادة موزعة على خمسة أبواب، تغطي كافة الجوانب المتعلقة باستخدام التوقيع والتصديق الإلكترونيين، بما في ذلك:

1. تحديد المفاهيم الأساسية،
2. الشروط الواجب توافرها في التوقيع الإلكتروني الموثوق،
3. تنظيم نشاط مقدمي خدمات التصديق الإلكتروني،
4. تحديد التزاماتهم وحقوقهم،
5. وكذا العقوبات المقررة عند الإخلال بالأحكام القانونية.

وقد ركز المشرع من خلال هذا الإطار على حماية أمن وسلامة الوثائق الإلكترونية وضمان موثوقيتها، بهدف تعزيز الثقة في التبادلات الرقمية، خصوصاً في ظل تنامي استخدام الوسائل الإلكترونية في الإدارة، التجارة، والخدمات العمومية.

### ثانياً: دوافع صدور الأمر 04-15 وسياقه

يسعى المشرع الجزائري إلى مواكبة التطورات التكنولوجية الحديثة في مجال الإدارة، حيث تشهد السنوات الأخيرة توجه غالبية المؤسسات والقطاعات الوزارية إلى التوجه نحو استخدام نظم إدارة الوثائق الإلكترونية. وعلى هذا الأساس بادر بإصدار القانون 04-15 المتعلق بالتوقيع والتصديق الإلكترونيين.<sup>1</sup>

<sup>1</sup> كحيلة سارة، مرجع سابق، ص 50

جاء القانون استجابة للتحويلات المتسارعة في مجال الرقمنة وتبادل المعلومات عبر الإنترنت، حيث أصبحت المؤسسات العمومية والخاصة تعتمد بشكل متزايد على التبادلات الإلكترونية. وكان من الضروري وضع إطار قانوني ينظم كيفية إثبات هذه المعاملات، ويضمن سلامتها وعدم إنكارها أمام الجهات المختصة.

كما استلهم القانون من الحاجة لضمان الثقة في الوثائق الإلكترونية، التي كثيراً ما يُطعن في صحتها بسبب سهولة نسخها أو التلاعب بها. فجاءت النصوص من المادة 6 إلى المادة 9 لتمنح التوقيع الإلكتروني القوة القانونية الكاملة، رفضه وتحضر رفضه كدليل مجرد كونه إلكترونياً. وقد تأثر المشرع الجزائري بتجارب الدول الرائدة في المجال، بالإضافة إلى المبادئ العامة للقانون الدولي، وخاصة تلك الواردة في "قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية"، مما يُبرز الطابع التوافقي لهذا القانون مع التشريعات المقارنة.

### ثالثاً: دور القانون 04-15 في حماية الوثيقة الإلكترونية<sup>1</sup>

1. مصداقية للوثائق الإلكترونية باعتبارها وثيقة رسمية.
2. حماية الوثائق الإلكترونية من التزوير والتحريف.
3. تحديد الجهات المسؤولة عن التصديق الإلكتروني.
4. اعتماد نظام قانوني للقيام بالتصديق الإلكتروني.
5. معاقبة كل من يقوم بتزوير أو إفشاء سرية البيانات المتعلقة بالتصديق الإلكتروني أو استعمالها لغير الأغراض التي منحت له.

### المطلب الثاني: الآليات التقنية الداعمة للإطار القانوني

تُعد الآليات التقنية عنصراً مكملاً وضرورياً للإطار القانوني، حيث تمثل الوسائل العملية التي تترجم الأحكام القانونية إلى تدابير فعالة لحماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، بما يعزز من مستوى الأمان المعلوماتي ويضمن الامتثال للمعايير التقنية والتنظيمية. وانطلاقاً من هذه الأهمية، سيتم التطرق في هذا المطلب إلى الآليات التقنية الأساسية الداعمة لهذا الإطار، من خلال معالجة إدارة الهوية والوصول، التشفير، والتوقيع الإلكتروني.

<sup>1</sup> زيدان فضيلة، مرجع سابق، ص 34

## الفرع الأول: إدارة الهوية والوصول

تُعد إدارة الهوية والوصول أحد الركائز الأساسية لحماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، حيث تسهم في ضمان أن الأشخاص المخولين فقط هم من يمكنهم الوصول إلى البيانات الحساسة. في هذا الفرع، سنتناول بالشرح آلية التحقق من الهوية وكيفية التحكم في الوصول إلى المعلومات.

## أولاً: التحقق من الهوية

تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص (أو الجهة) وأنه الشخص المعني لا غير. فعند اتصال شخصين (أو جهتين) ببعضهما البعض، فلا بد من أن يتعرف كل منهما إلى الآخر. لضمان أن يتعامل كل منهما مع الشخص أو الجهة المعنية وليس مع غيرها. بعبارة أخرى، فإن التحقق من الهوية هو التحقق من أن المستخدم المتقدم ما هو بالفعل من ادعى أنه ذلك المستخدم. وفي حال تزويد المعلومات، فإنه يجب التحقق من هوية المرسل لضمان أن المعلومة قادمة من مصدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة واصلت إلى وجهتها الصحيحة.<sup>1</sup>

تبدأ عملية التحقق من الهوية بالتعريف بالهوية أو تحديد الهوية. ويمكن تحقيق ذلك من خلال اسم المستخدم أو رقم الحساب مثلاً. ان تحديد هوية الشخص أو التعريف به رقمياً (إلكترونياً) أمر مهم، وقد يكون صعباً في بعض الأحيان؛ إذ إن الشخص الواحد نفسه قد يكون لديه أكثر من هوية رقمية. فمثلاً قد يكون لموظف واحد اسم مستخدم لأغراض العمل واسم مستخدم لأغراض تصفحه الخاصة بالإنترنت. لذا يجب ان تتوفر في طريقة تحديد الهوية المعايير التالية:

**1. أن تكون الهوية فريدة:** ومعنى ذلك أن تكون غير قابلة للتكرار، ومثال ذلك أن يكون للشخص رقم هوية فريد خاص به لا يشترك معه غيره فيه، ومثال آخر هو استخدام الخصائص الحيوية للإنسان، كبصمات الأصابع، ومسحات العين.

**2. أن تكون غير مفصحة:** عن معلومات المستخدم ووظيفته والغرض من وصوله إلى المعلومة، ومثال ذلك ألا يتم اسم المستخدم لنظام معين

<sup>1</sup> ذيب بن عايض القحطاني، أمن المعلومات، مطابع مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، السعودية، 2015، ص80

3. ألا تكون مشتركة بين المستخدمين: كإعطاء اسم كامل به عدد من الموظفين لاسم المستخدم نفسه.

4. إتباع معايير التسمية المعتمدة: عند إنشاء حسابات المستخدمين، كاستخدام أول حرف من اسم المستخدم متبوعاً ببقية اسم العائلة، أو غير ذلك من التنسيقات التي قد يستفاد منها في تحديد الشخص بسهولة عند إجراء عمليات التدقيق والمتابعة.<sup>1</sup>

### ثانياً: التحكم بالوصول

التحكم بالوصول هو مقدرة (أو وظائف) الحماية التي تتحكم بوصول المستخدمين أو الأنظمة إلى موارد المنشأة، كالأجهزة الرئيسية والبيانات المركزية، أو بعبارة أخرى منع الاستخدام غير المرخص به للموارد. فتلك الحقوق هي التي تحدد الأنشطة والموارد المتاحة المختلفة للمرخص له عند الوصول لشيء ما.

يأتي عنصر التحكم بالوصول بعد عنصر التحقق من الهوية. فعندما يتم التحقق من هوية الشخص ويُسمح له بالدخول إلى شبكة الحاسب الآلي مثلاً، فإنه يجري التحكم باستخدامه لموارد محددة من الشبكة. وليس جميع الموارد على طريق التحكم بالوصول، من أجل ذلك توجد قائمة التحكم بالوصول للموارد المهمة في الشبكة، والتي تحدد الأشخاص المصرح لهم فقط باستخدامها (وإن كان مصرحاً لهم بالدخول إلى الشبكة عموماً). وبشكل دقيق، فإنّ منح الاستخدام غير المرخص به لأي معلومة، وكذلك تحديد صلاحيات محددة للأشخاص المصرح لهم بالوصول إلى المعلومات؛ لاستخدامها والاطلاع عليها تحت شروط محددة. فيمكن أن يكون هناك أشخاص لهم صلاحية الاطلاع (القراءة) فقط، وآخرون لهم صلاحية الطباعة، وآخرون لهم صلاحية الحذف... وهكذا.<sup>2</sup>

تُعد إدارة الهوية والوصول عنصراً أساسياً في حماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، إذ تضمن أن الأشخاص المخولين فقط هم من يمكنهم الوصول إلى المعلومات الحساسة. من خلال التحقق الدقيق من هوية المستخدمين وتحديد صلاحياتهم بدقة، تسهم إدارة الهوية في تقليل مخاطر الاختراقات، وتسرب المعلومات، وضمان الامتثال للمعايير القانونية والتنظيمية.

<sup>1</sup> ذيب بن عايض القحطاني، مرجع سابق، ص 80-81.

<sup>2</sup> ذيب بن عايض القحطاني، نفس المرجع والصفحة سابقاً.

كما تساعد على تعزيز الثقة في البيئة الرقمية من خلال توفير طبقة حماية إضافية. وتعد إحدى أهم الآليات التقنية الداعمة للإطار القانوني لحماية المعلومات والوثائق الإلكترونية.

### الفرع الثاني: التشفير

تتراكم التهديدات والمخاوف من جرائم تهدد نظم المعلومات، مما استدعى الحاجة إلى خصوصية المعلومات وحماية البيانات السرية. ويمكن التشفير أن يعطي درجة عالية من الأمن بأقل كلفة، وتتوافر عمليات تطوير تقنيات جديدة في مجال التشفير بحيث تعطي مستويات أعلى من الأمن عند تطبيقها على نظام المعلومات، وفي ظل التطور المتسارع للحاسوب وشبكات الاتصال باتت الحاجة ملحة لطرق تشفير قوية، ومن مبررات ذلك لأن زيادة سرعة الكمبيوتر تعني تقصير الوقت الذي يحتاجه الكمبيوتر لكسر أو كشف مفتاح تشفير معين.<sup>1</sup>

ويعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح تصبح غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها، ويتم عادة تشفير البيانات قبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأي عمليات تجسس أو تحريف لمضمونها، على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة.<sup>2</sup>

يُعد التشفير من الوسائل التقنية لحماية المعلومات المصنفة والوثائق الإلكترونية، حيث يضمن سرية المعلومات المصنفة ويمنع الوصول غير المصرح به إليها. من خلال تحويل المحتوى إلى صيغة غير مفهومة إلا باستخدام مفاتيح معينة، يُصعب التشفير على المتسللين قراءتها أو استغلالها حتى في حال تمكنهم من الوصول إليها. وبالتالي، فإنه يعزز من مستوى الأمان المعلوماتي، ويحافظ على خصوصية البيانات، ويُعتبر خط الدفاع في مواجهة التهديدات الإلكترونية، خاصة في البيئات الحساسة التي تتطلب حماية صارمة للمعلومات.

<sup>1</sup> بغداد محمد، "الأمن المعلوماتي وسبل حمايته في الجزائر - دراسة حالة مؤسسة اتصالات الجزائر - سعيدة" - مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية تخصص تسيير وإدارة المنظمات الأمنية، جامعة سعيدة - الدكتور مولاي الطاهر، 2017-2018 ص 58

<sup>2</sup> فؤاد حبيب، وحنان كريبط، "أمن المعلومات ودوره في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة"، مجلة المؤسسة، جامعة الجزائر 3، العدد 3، 2014، ص 203

## الفرع الثالث: التوقيع الإلكتروني

إن التوقيع الإلكتروني عبارة عن حروف وأرقام أو رموز أو إشارات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتميزه عن غيره ، ويتم اعتماده من الجهة المختصة، ويعتمد بهذا التوقيع على قلم خاص يتم به التوقيع يدويا على شاشة الكمبيوتر أو على لوح رقمي، وعندئذ يتم تحليل التوقيع الخطي عن طريق الكمبيوتر وتخزينه كمجموعة من القيم الرقمية التي يمكن أن تضاف إلى رسالة البيانات، كما يمكن للمتلقي عرضها على شاشة الكمبيوتر للتوثيق، والتي من المفترض أن عينات من التوقيع الخطي قد سبق تخزينها وتحليلها بواسطة الأدوات الإحصائية.<sup>1</sup>

يعرف التوقيع الإلكتروني في المادة 2 الفقرة الأولى من القانون رقم 04-15 سالف الذكر بأنه: "بيانات إلكترونية في شكل إلكتروني، مضافة أو مرتبطة منطقيًا ببيانات إلكترونية أخرى تستعمل كوسيلة للتوقيع."<sup>2</sup>

ويتضح أن المشروع اعتمد في تعريفه على أشكال وإجراءات التوقيع الإلكتروني، وركز على أن تكون مرتبطة بما ورد في المحرر الإلكتروني الذي يحمله كما أشار إلى الغرض الأساسي للتوقيع الإلكتروني، وهو توثيق وقبول الموقع على ما ورد في المحرر الإلكتروني الموقع الكترونيا من طرفه.

التوقيع الإلكتروني يحمي الوثيقة الإلكترونية إلى درجة عالية من الموثوقية والمصادقية فهو يقوم على أرقام سرية تجعل رسائل البيانات المتبادلة مشفرة لا يمكن قراءتها ولا الوصول إليها الا الذي يحوز الرقم السري بشكل يضمن سرية وسلامة الوثيقة الإلكترونية.

## المطلب الثالث: الحماية المؤسسية

بالإضافة إلى الآليات التشريعية والتقنية، تكتسي الحماية المؤسسية أهمية بالغة في مواجهة التهديدات التي تستهدف المعلومات المصنفة والوثائق الإلكترونية، خصوصًا في ظل تطور أساليب الجريمة الإلكترونية وتعدد وسائل اختراق الأنظمة المعلوماتية. ولتحقيق نجاعة حقيقية في التصدي لهذه المخاطر، تبنت الدولة الجزائرية مقارنة وقائية وهيكلية تقوم على إنشاء وتفعيل أجهزة وهيئات مختصة

<sup>1</sup> بغدادي إيمان، "التوقيع الإلكتروني كبديل للتوقيع التقليدي في التجارة الإلكترونية"، مجلة الاقتصاد الدولي والعملة، جامعة قسنطينة 1، الجزائر، المجلد 2، العدد 4، 2019، ص18

<sup>2</sup> القانون رقم 04-15، مرجع سابق، ص6

في مجال أمن المعلومات والوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ولعل أن أبرز هذه الهيئات والأجهزة هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (الفرع الأول)، إضافة إلى وكالة امن الأنظمة المعلوماتية (الفرع الثاني)

### الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تعود فكرة إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إلى سنة 2009 تاريخ صدور القانون 09-04 المتعلق بتحديد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بحيث جاء في نص المادة 13 من القانون على أنه " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفية سيرها عن طريق التنظيم".<sup>1</sup>

وفي سنة 2015 صدر المرسوم الرئاسي رقم 15-261 الذي تضمن تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها<sup>2</sup> ثم الغي بموجب المرسوم الرئاسي رقم 19-172<sup>3</sup> ليتم بعد ذلك اعادة تنظيم الهيئة بموجب المرسوم الرئاسي 20-183<sup>4</sup> وهو المعتمد به حالياً.

### أولاً: تشكيل الهيئة وتنظيمها

تضم الهيئة مجلس توجيه ومديرية عامة تنقسم بدورها الى مديرية للمراقبة الوقائية واليقظة الإلكترونية ومديرية الادارة والوسائل ومصالحة للدراسات والتلخيص ومصالحة التعاون واليقظة التكنولوجية<sup>5</sup> حيث يرأس مجلس التوجيه رئيس الجمهورية او ممثله ويتشكل الوزير المكلف بالعدل

<sup>1</sup> المادة 13 من القانون 09-04 المؤرخ في 14 شعبان عام 1430 هـ الموافق ل 5 غشت سنة 2009، يحدد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47، الصادرة بتاريخ 25 شعبان عام 1430 هـ الموافق ل 16 غشت سنة 2009.

<sup>2</sup> المرسوم الرئاسي رقم 15-261، المؤرخ في 24 ذي الحجة عام 1436 هـ الموافق ل 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 53، الصادرة بتاريخ 24 ذي الحجة عام 1436 هـ الموافق ل 8 أكتوبر سنة 2015.

<sup>3</sup> المرسوم الرئاسي رقم 19-172، المؤرخ في 3 شوال عام 1440 هـ الموافق ل 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر.ج.ج، العدد 37، الصادرة بتاريخ 6 شوال عام 1440 هـ الموافق ل 9 يونيو سنة 2019.

<sup>4</sup> المرسوم الرئاسي رقم 20-183، المؤرخ في 21 ذو القعدة عام 1441 هـ الموافق ل 13 يوليو سنة 2020، يتضمن اعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 40، الصادرة بتاريخ 26 ذو القعدة عام 1441 هـ الموافق ل 18 يوليو سنة 2020.

<sup>5</sup> المادة 11 من المرسوم الرئاسي رقم 20-183، نفس المرجع.

والوزير المكلف بالداخلية والوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والمدير العام للأمن الداخلي وقائد الدرك الوطني والمدير العام للأمن الوطني وممثل عن رئاسة الجمهورية وممثل عن وزارة الدفاع الوطني.<sup>1</sup>

يكلف مجلس التوجيه على الخصوص بتوجيه عمل الهيئة والإشراف عليه ومراقبته ودراسة كل مسألة تخضع لمجال اختصاص الهيئة لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 04-09 المؤرخ في 5 أوت سنة 2009، بالإضافة إلى ذلك تختص الهيئة بضبط برنامج عمل الهيئة وتحديد شروط وكيفيات تنفيذه والقيام دوريا بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، واقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ودراسة مشروع النظام الداخلي والموافقة عليه.<sup>2</sup>

وتعنى المديرية العامة بالسهر على السير الحسن للهيئة، وتعد مشروع ميزانيتها وتعرضه على مجلس التوجيه، كما تتولى إعداد وتنفيذ برنامج العمل بعد المصادقة عليه، وتنسق جهود الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتتكفل بجمع وتبادل المعلومات مع الهيئات الدولية بهدف تحديد هوية مرتكبي هذه الجرائم. كما تمثل المديرية الهيئة أمام السلطات الوطنية والدولية، وتشرف على تأهيل المستخدمين وأداء اليمين القانونية، وتسهر على التسيير الإداري والمالي، وتحضير اجتماعات مجلس التوجيه، وإعداد التقرير السنوي لنشاطات الهيئة لعرضه للمصادقة.<sup>3</sup>

### ثانيا: مهام الهيئة

بالرجوع إلى المادة 14 من القانون 04/09 نجد أن مهام هذه الهيئة تتمثل في:

1. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

<sup>1</sup> المادة 6 من المرسوم الرئاسي رقم 20-183، مرجع سابق.

<sup>2</sup> المادة 7 من المرسوم رقم 20-183، نفس المرجع.

<sup>3</sup> المادة 10 من المرسوم 20-183، نفس المرجع.

2. مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

3. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم<sup>1</sup>.

أما من خلال أحكام المرسوم الرئاسي 20-183 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إضافة إلى المهام المسندة لها بموجب أحكام القانون 09/04 المشار إليه سابقا تكلف الهيئة على الخصوص ووفقا لنص المادة 04 منه بما يأتي<sup>2</sup>:

1. اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

2. تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

3. مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية.

4. ضمان المراقبة الوقائية للاتصالات الإلكترونية.

5. تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

6. السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

7. المساهمة في تكوين المحققين المتخصصين في مجال لتحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

<sup>1</sup> المادة 13 من القانون 09-04، مرجع سابق.

<sup>2</sup> المادة 4 من المرسوم الرئاسي 20-183، مرجع سابق.

## الفرع الثاني: وكالة امن الأنظمة المعلوماتية

في ظل تزايد الاعتماد على النظم المعلوماتية في تداول وتخزين الوثائق والمعلومات المصنفة، أصبحت الحاجة ماسة إلى وجود جهاز تقني متخصص يُعنى بأمن الأنظمة المعلوماتية على المستوى الوطني. وفي هذا السياق، جاء المرسوم الرئاسي رقم 20-05 يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.<sup>1</sup> والتي تشمل المجلس الوطني لأمن الأنظمة المعلوماتية ووكالة أمن الأنظمة المعلوماتية (ANSI)، والتي أنشئت لضمان أمن البنى التحتية المعلوماتية وحماية المعطيات الحساسة، لا سيما تلك التي تندرج ضمن المعلومات المصنفة.

## أولاً: تنظيم وكالة امن الأنظمة المعلوماتية وسيرها

يتولى إدارة الوكالة لجنة توجيه وتزود بلجنة علمية، كما يكلف بتسييرها مدير عام، وتتوفر على مركز وطني عملياتي لأمن الأنظمة المعلوماتية ومديريات ومصالح تقنية وإدارية موضوعة تحت سلطته.<sup>2</sup>

تتكون لجنة التوجيه من ممثلي وزارة الدفاع الوطني، الوزارة المكلفة بالشؤون الخارجية، الوزارة المكلفة بالداخلية، الوزارة المكلفة بالعدل، الوزارة المكلفة بالمالية، الوزارة المكلفة بالطاقة، الوزارة المكلفة بالتعليم العالي، الوزارة المكلفة بالصناعة، الوزارة المكلفة بالاتصالات، الوزارة المكلفة بالتجارة، مصالح الأمن، سلطة ضبط البريد والاتصالات الإلكترونية، السلطة الوطنية للتصديق الإلكتروني، الهيئة الوطنية لحماية البيانات ذات الطابع الشخصي، السلطة الحكومية للتصديق الإلكتروني، وعلى سبيل الاستشارة، المدير العام للوكالة، على أن تتولى مصالح الوكالة أمانة لجنة التوجيه. كما يمكن أن تستعين لجنة التوجيه بأي شخص أو مؤسسة من شأنها تنويرها في أعمالها.<sup>3</sup> وتشرف اللجنة بدورها على اقتراح الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، المصادقة على البرامج التنفيذية، وتقييم نتائج الوكالة، إلى جانب ضبط الاحتياجات الوطنية في المجال وتسيير الجوانب الإدارية والمالية للوكالة.<sup>4</sup>

<sup>1</sup> المرسوم الرئاسي رقم 20-05، المؤرخ في 24 جمادى الأولى عام 1441هـ الموافق لـ 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، ج.ر.ج.ج، العدد 04، الصادرة بتاريخ أول جمادى الثانية عام 1441هـ الموافق لـ 26 جانفي سنة 2020.

<sup>2</sup> المادة 20 من المرسوم الرئاسي رقم 20-05، نفس المرجع.

<sup>3</sup> المادة 22 من المرسوم 20-05، نفس المرجع.

<sup>4</sup> المادة 24 المرسوم 20-05، نفس المرجع.

أما المدير العام، فيُعين وفقاً لتنظيم وزارة الدفاع، ويتولى تنفيذ الاستراتيجية الوطنية، وإعداد البرامج ومشاريع الميزانية، وإبرام العقود، ويمثل الوكالة أمام القضاء، كما يشرف على المستخدمين وسير الوكالة وفق القوانين المعمول بها.<sup>1</sup>

وتتكوّن اللجنة العلمية من خبراء وأساتذة تُعيّنهم لجنة التوجيه، وتُعنى بإبداء الرأي حول البرامج العلمية والبحثية، والمشاركة في التظاهرات العلمية، والتكوين، والتأهيل في مجال أمن الأنظمة المعلوماتية، ولها صلاحية الاستعانة بخبراء لدعم مهامها.<sup>2</sup>

### ثانياً: مهام وكالة أمن الأنظمة المعلوماتية

تكلف الوكالة بموجب المادة 18 على الخصوص بما يأتي:

1. تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.
2. تنسيق تنفيذ الاستراتيجية الوطنية في مجال لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.
3. اقتراح كفاءات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.
4. إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية.
5. السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.
6. متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.
7. تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع استراتيجية أمن الأنظمة المعلوماتية.
8. ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية.
9. مرافقة الإدارات والمؤسسات والهيئات، بالتشاور مع الهياكل المختصة في هذا المجال في معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية، بعد الرأي المطابق للمجلس.
10. اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها.
11. اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني.
12. القيام بنشاطات التكوين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية.
13. تقديم توجيهات تتعلق بتكوين أعوان المؤسسات العمومية في مجال أمن الأنظمة المعلوماتية.

<sup>1</sup> المادة 28 المرسوم 05-20، مرجع سابق.

<sup>2</sup> المواد 31.32 من المرسوم 05-20، نفس المرجع.

### المبحث الثاني: الآليات الجزائية لحماية المعلومات المصنفة والوثائق الإلكترونية

تزايد أهمية الحماية الجزائية للمعلومات والوثائق الإلكترونية في ظل التطورات التكنولوجية المتسارعة والتهديدات المتزايدة التي تواجه الأنظمة المعلوماتية، مما يتطلب تعزيز الإجراءات القانونية لحمايتها. يعد الأمر 09-21 إطاراً قانونياً مهماً في الجزائر، حيث يحدد قواعد الحماية الجزائية لهذه المعلومات والوثائق، من خلال معاقبة الأفعال التي تُهدد أمن وسلامة الوثائق المصنفة والمعلومات الحساسة.

يهدف هذا المبحث إلى دراسة مختلف الجرائم التي تمس المعلومات والوثائق الإلكترونية، سواء كانت تقليدية أو معلوماتية، وتوضيح الأركان الجزائية لكل جريمة والعقوبات المرتبطة بها. سيتم التركيز على الجرائم التي تقع على المعلومات والوثائق المصنفة في النظام الجزائي الجزائري، مع تسليط الضوء على التعديلات المستحدثة في ظل تكنولوجيا المعلومات.

#### المطلب الأول: الجرائم التقليدية الواقعة على المعلومات المصنفة والوثائق الإلكترونية

يمكن أن تكون الوثائق والمعلومات الإدارية محلاً لأفعال إجرامية تمس بسريتها وسلامتها، خاصة من قبل أشخاص مؤتمنين عليها بحكم وظائفهم. وقد خصص المشرع الجزائري ضمن الأمر 09-21 عدة أحكام تُجرّم الأفعال التي تمس بحماية الوثائق المصنفة سواء تعلق الأمر بالإفشاء، الإخفاء، التزوير، أو الامتناع عن تسليمها. وتُعد هذه الجرائم تقليدية لأنها تقع في إطار مادي ملموس، رغم إمكانية تكييفها لاحقاً بوسائل رقمية.

#### الفرع الأول: إفشاء ونشر الوثائق والمعلومات المصنفة

يلتزم الموظف العمومي وغيره بحماية المعلومات والوثائق الإدارية المصنفة تحت طائلة المسؤولية الجزائية، حيث جرم الأمر 09-21 بعض السلوكيات التي تشكل إخلالاً جسيماً بهذه الالتزامات، تتمثل فيما يلي:

<sup>1</sup> المادة 18 من المرسوم 05-20، نفس المرجع.

## أولاً: جريمة إفشاء المعلومات والوثائق الإدارية المصنفة

إفشاء المعلومات والوثائق الإدارية المصنفة هي جنحة، إضافة للركن المفترض أي أن يكون الجاني موظفاً، تقوم هذه الجريمة على:

**1. الركن المادي:** قيام الموظف العمومي بإفشاء أو إطلاع الغير على معلومة أو وثيقة مصنفة أو السماح له بأخذ صورة منها، ماعدا في الحالات التي يسمح القانون بذلك ويتحقق كذلك الفعل الإجرامي أيضاً في حال الإهمال أو التساهل في حفظ هذه الوثائق، بما يؤدي إلى اطلاع غير المخولين عليها.

**2. الركن المعنوي:** هي جريمة لا يشترط لقيامها القصد الجنائي للموظف، لكنه يؤثر على العقوبة الموقعة، فالمشرع شدد في العقوبة في حالة الإفشاء العمدي، على النحو التالي:

### أ) الإفشاء العمدي للمعلومات والوثائق الإدارية المصنفة:

تختلف عقوبة هذه الجريمة حسب تصنيف المعلومات والوثائق الإدارية محل الإفشاء إلى ثلاثة حالات:

- **الحالة الأولى:** عندما يقع الإفشاء على معلومة أو وثيقة مصنفة توزيع "محدود" فيعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 60.000 دج إلى 300.000 دج. وشدد العقوبة إلى الحبس من سنة إلى خمس سنوات وبغرامة من 100.000 دج إلى 500.000 دج إذا مس الإفشاء بالاعتبار الواجب للسلطات العمومية.<sup>1</sup>
- **الحالة الثانية:** تكون عندما يتم إفشاء معلومة أو وثيقة مصنفة "واجب الكتمان" يعاقب الموظف الجاني بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000 دج إلى 500.000 دج.
- **الحالة الثالثة:** عندما تكون معلومة أو وثيقة مصنفة "سري" أو "سري" "جدا محل الإفشاء فتكون العقوبة بالحبس من خمس إلى عشر سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج.<sup>2</sup>

### ب) الإفشاء غير العمدي للمعلومات والوثائق الإدارية المصنفة:

<sup>1</sup> المادة رقم 28، الأمر -21-09، مرجع سابق

<sup>2</sup> المادة رقم 29، الأمر -21-09، نفس المرجع.

يعني تسبب الموظف في إفشاء معلومة أو وثيقة مصنفة بسبب عدم مراعاته للأحكام التشريعية و/أو التنظيمية أو القواعد الاحترازية المرتبطة بطبيعة مهامه أو وظيفته، فإذا كانت المعلومة أو الوثيقة مصنفة "توزيع محدود" يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 30.000 دج إلى 100.000 دج، أما إذا كان تصنيفها واجب الكتمان "أو "سري" أو "سري جدا" تكون العقوبة بالحبس من ستة أشهر إلى سنتين و/أو بغرامة من 60.000 دج إلى 200.000 دج.<sup>1</sup>

### ثانيا: جريمة إفشاء الأسرار المهنية

إفشاء الأسرار المهنية جنحة، يعاقب مرتكبها بالحبس من ثلاث إلى خمس سنوات وبغرامة 300.000 دج إلى 500.000 دج، تقوم بالإضافة إلى الركن المفترض على ان يكون الجاني موظفا على:

**1. الركن المادي:** يتجسد الركن المادي لهذه الجريمة من خلال قيام الجاني، وهو شخص مؤتمن على السر المهني، بكشف أو إفشاء معلومات أو وقائع أو وثائق تُعد بطبيعتها أو بنص القانون من الأسرار المهنية. هذا الإفشاء قد يتم عن طريق التصريح الشفوي، أو الكتابة، أو حتى عبر وسائط إلكترونية، ويكفي فيه أن يتم الكشف للغير، أي لشخص غير محول له الاطلاع على تلك المعطيات. وتجدر الإشارة إلى أن الجريمة تقوم حتى وإن لم يترتب عن الإفشاء أي ضرر فعلي، لأن مجرد الإخلال بالواجب المهني في حد ذاته يُعد فعلاً مجرمًا.

**2. الركن المعنوي:** أما من حيث الركن المعنوي، فتُصنف جريمة إفشاء الأسرار المهنية ضمن الجرائم العمدية، التي يشترط فيها توافر القصد الجنائي العام. ويتحقق هذا القصد من خلال علم الجاني بأن المعلومات التي قام بإفائها هي معلومات سرية يحظر القانون الكشف عنها، وأنه مع ذلك اتجهت إرادته إلى نشرها أو إفشائها، سواء بدافع الانتقام، أو الإهمال المتعمد، أو لتحقيق مصلحة شخصية، أو بدافع الفضول. ولا يُشترط أن تكون لدى الجاني نية الإضرار بالغير، بل يكفي أن يتم الإفشاء مع توافر العلم والإرادة، أي أن الجاني تصرف عن وعي وإرادة في مخالفة واجب التحفظ.

### ثالثا: جريمة نشر وثائق التحقيق القضائي

<sup>1</sup> المادة رقم 31، الأمر -21-09، مرجع سابق.

نشر وثائق التحقيق القضائي جنحة، يعاقب كل شخص ارتكبها لعقوبة الحبس من ثلاث إلى خمس سنوات وبغرامة من 300.000 دج إلى 500.000 دج<sup>1</sup>، تقوم على:

**1. الركن المادي:** نشر أو إفشاء محتوى محاضر و/أو أوراق التحقيق أو التحري القضائي، أو تمكين مثلاً صفة له بالحصول عليها، وهو السلوك الذي يخالف مبدأ سرية التحقيق القضائي، الذي يمنع وصول غير الأطراف لهذه المعلومات والوثائق.

**2. الركن المعنوي:** فإن هذه الجريمة تُعد من الجرائم العمدية التي لا تقوم إلا إذا توافرت النية الجنائية لدى الجاني. ويُقصد بذلك أن يكون الشخص الذي قام بالفعل عالماً بأن الوثائق التي ينشرها تتعلق بتحقيق قضائي، وأنها مشمولة بسرية قانونية، ومع ذلك يقدم على نشرها أو تسريبها بإرادة حرة واختيار واعٍ. ولا يُشترط في هذا الإطار أن يكون هدف الجاني التأثير على التحقيق أو تحقيق مصلحة شخصية، بل يكفي ثبوت العلم والإرادة في خرق مبدأ السرية، وهو ما يميز القصد الجنائي في مثل هذه الجرائم.

### الفرع الثاني: الحيابة والتعدي على المعلومات والوثائق المصنفة

من خلال هذا الفرع سنوضح الجرائم التي تتعلق بحيابة الوثائق المصنفة بدون حق أو إخفاء الوثائق أو إتلافها أو تزويرها. كما يعرض القانون الجزائري العقوبات المرتبطة بهذه الجرائم وفقاً للقواعد المعمول بها في قانون حماية الوثائق الإدارية.

#### أولاً: جنحة إخفاء الوثائق المصنفة أو إتلافها أو تزويرها

عالج المشرع الجزائري واقعة إخفاء الوثائق المصنفة أو الأشياء أو أدوات الجريمة التي استعملت في ارتكاب الجرائم المنصوص عليها في هذا القانون وعائدات الجريمة من أموال أو أشياء أخرى في المادة 36 من القانون 09 21، والقيام بهذه الأفعال الإجرامية من قبل الجاني لأجل طمس الحقيقة وتعطيل سير العدالة هذا من جهة. ومن جهة أخرى قد تقع هذه الجريمة أيضاً عن طريق ارتكاب أفعال إجرامية أخرى كاختلاس، أو التزييف العمدي لوثيقة عمومية من شأنها تسهيل عملية البحث عن الجرائم المنصوص عليها في هذا القانون. وهي كلها جرائم معاقب عليها بالمادة 36 المذكورة أعلاه

<sup>1</sup> المادة 32 من الأمر 09-21، مرجع سابق.

بالحبس من سنة (1) واحدة إلى خمس (5) سنوات وبغرامة 100.000 دج إلى 500.000 دج.<sup>1</sup>

ثانيا: جريمة حيازة وثيقة مصنفة والامتناع عن تسليمها

طبقا لأحكام المادة 35 من القانون رقم 09-21 تتحقق جريمة حيازة وثيقة مصنفة بتوافر ركنها المادي والمعنوي، ويقوم الركن المادي لهذه الجريمة بحيازة وثيقة مصنفة دون أن يكون مؤهلا لذلك ويعلم أنها وثيقة مصنفة، ولم يسلمها إلى السلطات المعنية، فالمشرع أضفى صبغة العمومية حين استعمل كلمة كل في العبارة "كل من يجوز وثيقة مصنفة" وبالتالي هذه الجريمة ترتكب من طرف الجميع سواء كان موظفاً أو من يدخل في حكمه أو من الغير، فإن لم يقم بتسليمها إلى السلطات المعنية يكون متعمداً وبالتالي يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج أو بإحدى هاتين العقوبتين هذا إذا لم يقم بإفشائها. أما إذا قام بإفشاء مضمون الوثيقة المصنفة التي بحوزته، تطبق عليه العقوبات المنصوص عليها في المادتين 28 و29 من نفس القانون حسب كل حالة. كما عاقبت المادة 40 من نفس القانون كل من يمتنع عن تقديم الوثائق المنصوص عليها في المادة 24 من القانون رقم 09/21 بالحبس من ثلاث (3) سنوات إلى خمس (5) سنوات وبغرامة من 300.000 دج إلى 500.000 دج.<sup>2</sup>

**المطلب الثاني: الجرائم المعلوماتية الواقعة على المعلومات المصنفة والوثائق الالكترونية**

مع التحول الرقمي الذي يشهده العالم وتزايد الاعتماد على تكنولوجيات الإعلام والاتصال، ظهرت أنماط جديدة من الجرائم لم تكن معروفة من قبل، باتت تهدد سلامة وسرية الوثائق الإدارية المصنفة. وقد استجاب المشرع الجزائري لهذا التطور من خلال تجريم أفعال معينة مستحدثة مثل الدخول غير المشروع إلى الأنظمة المعلوماتية، أو إنشاء مواقع إلكترونية بهدف نشر الوثائق المصنفة، وهي جرائم ذات طبيعة رقمية تتطلب وسائل فنية لارتكابها، وتتميز بطابعها التقني.

**الفرع الأول: جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية**

ان جريمة الدخول غير المشروع إلى الأنظمة المعلوماتية تعد من الجرائم التقنية المستحدثة، وقد اعتبرها المشرع الجزائري من الجرائم التي يُعاقب عليها حتى في غياب الضرر المباشر، لما تشكله من تهديد لأمن المعلومات. سنتناول في هذا الفرع الإطار القانوني لهذه الجريمة والعقوبات المقررة لها.

<sup>1</sup> تومي يحيى، "الحماية القانونية للمعلومات والوثائق الإدارية على ضوء القانون رقم 09-21: دراسة تحليلية"، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة احمد بن يحيى، تسمسليت، الجزائر، مجلد 7، عدد 2، 2022، ص16.

<sup>2</sup> تومي يحيى، نفس المرجع، ص17

## أولاً: أركان الجريمة

تضمنت جريمة الدخول الغير مشروع إلى منظومة معلوماتية قصد الاستيلاء على وثائق مصنفة بموجب أحكام المادة 37 من الأمر 09.21 السالف الذكر حيث ذكرت " دون الإخلال بالعقوبات الأشد، يعاقب كل من يدخل دون ترخيص إلى منظومة معلوماتية أو موقع الكتروني أو شبكة الكترونية أو أي وسيلة أخرى من وسائل تكنولوجيايات الإعلام والاتصال للسلطات المعنية، بقصد الحصول بغير حق على معلومات أو وثائق مصنفة."

وتجدر الإشارة إلى أن جريمة الدخول بطريق الغش إلى منظومة معلوماتية هي جريمة قائمة بذاتها حتى وإن لم يترتب عنها أي ضرر أو نتيجة، فهي من الأفعال الشكلية التي تقوم بمجرد السلوك وقد تناولها المشرع الجزائري في المادة 394 مكرر من قانون العقوبات<sup>1</sup> والتي تعنى بجرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي هي عبارة نظام معلوماتي يسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها الى معلومات.<sup>2</sup> وتقوم هذه الجريمة على الأركان التالية:

**1. الركن المادي:** تتحقق جريمة الدخول الغير مشروع إلى نظام معلوماتي بهدف الاستيلاء على وثائق مصنفة بمجرد قيام الفاعل بفعل الدخول غير المصرح به. ويشمل ذلك استخدام الوسائل التقنية للوصول إلى المعلومات. تعتبر الجريمة واقعة بفعل الدخول ذاته، بصرف النظر عن نجاح الاستيلاء أو النشر اللاحق للوثائق للإضرار أو تحقيق منافع شخصية. وبطال هذا التجريم أي نظام معلوماتي أو أي وسيلة اتصال إلكترونية.

**2. الركن المعنوي:** تعد هذه الجريمة عمدية، وتتطلب توافر القصد الجنائي بعنصره: العلم والإرادة. يجب أن يكون الفاعل عالماً بعدم أحقيته في الدخول إلى النظام المعلوماتي وأن تتجه إرادته نحو ارتكاب هذا الفعل. بالإضافة إلى ذلك، يشترط القانون قصداً جنائياً خاصاً يتمثل في نية الغش، والتي تتحقق بعلم الفاعل بعدم مشروعية الدخول وإقدامه عليه مع ذلك، سواء أتم الاستيلاء على الوثائق المصنفة أم لا.

<sup>1</sup> أنظر القانون رقم 24-06 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق لـ 8 يونيو سنة 1966 والمتضمن قانون العقوبات الصادر بـ ج.ر.ج. عدد 30 في 30 أبريل 2024.

<sup>2</sup> حابت آمال، الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 15.04 و 04.09، مجلة هيرودوت للعلوم الإنسانية والاجتماعية جامعة 8 ماي 1945، قالمة، الجزائر، المجلد 7، العدد 25، 2023، ص 56

## ثانيا: العقوبات المقررة

لقد نصت المادة 37 من الأمر 09-21 المشار إليه أعلاه على هذه الجريمة واعتبرتها  
جنحة مشددة، وحددت لها العقوبة التالية:<sup>1</sup>

- الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى  
1.000.000 دج.

- الحبس من عشر (10) سنوات إلى عشرين (20) سنة، وبغرامة من 1.000.000 دج إلى  
2.000.000 دج، عندما يكون نشر هذه المعلومات أو الوثائق المصنفة قصد الإضرار  
بالسلطات المعنية أو الحصول على منافع مباشرة أو غير مباشرة والملاحظ أن المشرع هنا لم  
يحدد طبيعة المنافع فقد تكون أموالا أو غيرها.

كما نصت المواد 394 مكرر من قانون العقوبات على هذه الجريمة وحددت لها العقوبات التالية:

- يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى  
200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة  
للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة.

## الفرع الثاني: جريمة إنشاء منظومة معلوماتية بقصد نشر المعلومات والوثائق المصنفة

يمثل إنشاء أو تسيير منصات معلوماتية بهدف نشر وثائق ومعلومات مصنفة انتهاكاً  
صارحاً لقواعد الحماية القانونية للمعلومات الحساسة، ويكشف عن نية جنائية واضحة في الإضرار  
بالمصلحة العامة. القانون الجزائري يواجه هذا الفعل بعقوبات حازمة ردعاً لمرتكبيه. في هذا الفرع،  
سنتعرض لمختلف جوانب هذه الجريمة من حيث التكييف القانوني والعقوبات المقررة.

## أولاً: أركان الجريمة

نص عليها المشرع الجزائري في الأمر 09-21-السالف الذكر من خلال نص المادة  
38 فقرة الأولى على جريمة إنشاء منظومة معلوماتية بقصد نشر المعلومات والوثائق المصنفة بقولها:  
"دون الإخلال بالعقوبات الأشد، يعاقب كل من ينشئ أو يدير أو يشرف على موقع الكتروني

<sup>1</sup> المادة 37 من الأمر 09-21، مرجع سابق

أو حساب إلكتروني أو برنامج معلوماتي يستعمل لنشر المعلومات أو الوثائق المصنفة أو محتواها كلياً أو جزئياً".<sup>1</sup>

**1. الركن المادي:** تتحقق هذه الجريمة بفعل إنشاء أو إدارة أو الإشراف على موقع إلكتروني، حساب إلكتروني، أو برنامج معلوماتي يُستخدم تحديداً لنشر معلومات ووثائق مصنفة. يشمل ذلك تصميم الموقع وتولي مسؤولية إدارته، تقوم الجريمة عند إنشاء واستخدام هذا النظام المعلوماتي بهدف نشر تلك المعلومات والوثائق السرية أو محتواها.

**2. الركن المعنوي:** يتطلب الركن المعنوي توافر القصد الجنائي، أي الإرادة الجرمية لدى الفاعل وعلمه التام بكافة عناصر الجريمة. يجب أن يكون الجاني على علم بأن المعلومة أو الوثيقة الإدارية تتمتع بالسرية، ومع ذلك تتجه إرادته إلى نشرها عبر منظومة معلوماتية.<sup>2</sup>

#### ثانياً: العقوبات المقررة:

ذكرت هذه الجريمة في نص المادة 38 من الأمر 09-21 السالفة الذكر، واعتبرتها جنحة مشددة وقد جعلت لها العقوبة التالية:

- الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج.<sup>3</sup>

#### الفرع الثالث: جريمة نشر المعلومات والوثائق المصنفة بواسطة منظومة معلوماتية

#### أولاً: أركان الجريمة

يُعد نشر المعلومات أو الوثائق الإدارية ذات الطابع السري عبر الوسائط الإلكترونية فعلاً مجرمًا إذا ما تم بهدف زعزعة النظام العام أو المساس بأمن الدولة، وهو ما يجعل هذه الجريمة في صلب الجرائم السيبرانية الحديثة. سنتوقف في هذا الفرع عند تحليل طبيعة هذا الفعل الإجرامي وأثره القانوني والجزاءات المرتبطة به.

<sup>1</sup> مريم ثابت، مرجع سابق، ص 34

<sup>2</sup> مريم ثابت، نفس المرجع، ص 35

<sup>3</sup> المادة 38 من الأمر 09-21، مرجع سابق

لقد نصت على جريمة نشر معلومات ووثائق إدارية بواسطة منظومة معلوماتية المادة 38 فقرة 2 من الأمر 09-21 المتعلق بحماية المعلومات والوثائق الإدارية والتي جاء فيها: "ويعاقب بنفس العقوبة كل من ينشر المعلومات والوثائق المصنفة أو محتواها كلياً أو جزئياً على شبكة إلكترونية أو بإحدى وسائل تكنولوجيات الإعلام والاتصال".<sup>1</sup>

كما شددت المادة 39 من عقوبة فعل النشر إذا كان الغرض منه المساس بالنظام العام والسكينة العامة.

وتبعاً لذلك تقوم الجريمة على الأركان التالية:

**1. الركن المادي:** يقوم الركن المادي لجريمة نشر معلومات ووثائق إدارية بواسطة منظومة معلوماتية على العناصر التالية:

- **فعل النشر:** يقصد به على النحو الذي تم الإشارة إليه بأنه هو الكشف عن المعلومات والوثائق الإدارية وإذاعتها بأي وسيلة من الوسائل، يعني أن جوهره هو نقل المعلومات والإفشاء بها للغير.

- أن يتم فعل النشر عن طريق الشبكة الإلكترونية أو بإحدى وسائل الإعلام والاتصال.<sup>2</sup>

**2. الركن المعنوي:**<sup>3</sup> جريمة نشر معلومات ووثائق إدارية بواسطة منظومة معلوماتية جريمة عمدية يشترط لقيامها توافر القصد الجنائي العام المتمثل في علم الجاني جريمة عمدية يشترط لقيامها توافر القصد الجنائي العام المتمثل في علم الجاني بسرية المعلومة والوثيقة الإدارية واتجاه إرادته إلى نشرها.

بينما إذا ارتبط الأمر بالفعل المنصوص عليه في المادة 39 من الأمر 09-21 المتعلق بحماية المعلومات والوثائق الإدارية فيشترط توافر قصد جنائي خاص يتمثل في نية الجاني إلى المساس بالنظام العام والسكينة العامة عند قيامه بفعل النشر

### ثانياً: العقوبات المقررة

نصت على هذه الجريمة أحكام المادة 38 فقرة 2 من الأمر 09-21 السالف الذكر وكذا المادة 39 منه، وقد اعتبرتها أيضاً جنحة مشددة، وأدرجت لها العقوبة التالية:

<sup>1</sup> المادة 38 فقرة 2 من الأمر 09-21، مرجع سابق.

<sup>2</sup> مريم ثابت، مرجع سابق، ص 35

<sup>3</sup> مريم ثابت، نفس المرجع، ص 36

- الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج.<sup>1</sup>
- الحبس من عشر (10) سنوات إلى خمس عشر (15) سنة وبغرامة من 1.000.000 دج إلى 1.500.000 دج. وذلك عندما يقوم الجاني عمدا بنشر أو بث المعلومات والوثائق الإدارية عن طريق منظومة معلوماتية بغرض المساس بالنظام العام والسكينة العامة.<sup>2</sup>

<sup>1</sup> المادة 38، فقرة 2 من الأمر 09-21، مرجع سابق

<sup>2</sup> المادة 39 من الأمر 09-21، نفس المرجع

اتضح لنا من خلال هذا الفصل أنّ حماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية ليست مجرد خيار، بل ضرورة حتمية تفرضها تحديات العصر الرقمي. وقد أظهر التحليل أنّ المشرّع الجزائري لم يغفل عن هذه المسألة، إذ سعى إلى وضع منظومة قانونية متكاملة تتضمن آليات وقائية وأخرى جزائية، بهدف تعزيز أمن المعلومات وحماية المعطيات الحساسة من أي اختراق أو استغلال غير مشروع.

ففي جانب الوقاية، تم التركيز على جملة من الإجراءات التقنية والتنظيمية التي تُسهم في تقليص المخاطر وتحسين الوثائق الإلكترونية ضد أي تهديد خارجي أو داخلي. أما في الجانب الجزائي، فقد تم تقنين مجموعة من الجرائم المعلوماتية التي ترتبط باستخدام تقنيات المعلومات في المساس بسرية وأمن الوثائق المصنفة، مقررًا لها عقوبات تتفاوت بحسب طبيعة وخطورة الأفعال المرتكبة.

ومجمل القول، فإن فعالية الحماية القانونية تبقى رهينة بمدى تكامل هذه الآليات من جهة، ومدى وعي المؤسسات والأفراد بأهمية احترام الإطار القانوني والتنظيمي من جهة أخرى، وهو ما يستدعي تعزيز الثقافة القانونية الرقمية وتطوير البنية التشريعية بما يتماشى مع التطورات المتسارعة في مجال تكنولوجيا المعلومات.

خاتمة

وختاماً يمكننا القول أن هذه الدراسة سعت من خلال فصلها، إلى تسليط الضوء على الإطار المفاهيمي والقانوني للمعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، بالإضافة إلى استعراض الآليات القانونية لحمايتها. وقد أظهر الفصل الأول "الإطار المفاهيمي للمعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية" أن التحول الرقمي قد فرض واقعاً جديداً يتسم بالديناميكية والتفاعلية، مما استدعى تعريفاً وتصنيفاً دقيقاً للمعلومات المصنفة والوثائق الإلكترونية في ظل بيئة رقمية تتسم بالحدثة والتطور المستمر.

وفي سياق متصل، تناول الفصل الثاني "الآليات حماية لمعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية" الدور المحوري للمشرع الجزائري في وضع منظومة قانونية متكاملة. وقد اتضح أن هذه المنظومة لم تقتصر على الجانب الوقائي من خلال الإجراءات التشريعية، تقنية ومؤسسية، والتي تسهم في تقليص المخاطر وتحسين الوثائق الإلكترونية، بل امتدت لتشمل آليات جزائية صارمة تهدف إلى معاقبة الجرائم المرتبطة باختراق أو نشر أو استغلال هذه البيانات بطرق غير مشروعة، مما يعكس حرص المشرع على تعزيز الأمن المعلوماتي وحماية المعطيات الحساسة التي تمس الأمن والنظام العام.

وعليه يمكن القول إن المشرع الجزائري قد أبان عن وعي كبير بالتحديات التي تفرضها البيئة الرقمية، وسعى جاهداً لتوفير حماية قانونية شاملة. فمن خلال الدمج بين الإجراءات الوقائية والعقوبات الجزائية المشددة، تبين الرؤية التشريعية التي تهدف إلى تحقيق أقصى درجات الحماية لهذا النوع من المعلومات والوثائق.

وقد توصلنا من خلال الدراسة إلى النتائج التالية:

- البيئة الرقمية خلقت واقعاً جديداً يتطلب تكييفاً قانونياً وتقنياً دقيقاً لحماية الوثائق والمعلومات المصنفة.
- المشرع الجزائري استحدث من خلال الأمر 09-21 والقانون 04-15 منظومة قانونية متقدمة نسبياً، تُعنى بحماية هذه الوثائق من خلال التصنيف، التقييد، والعقوبات.

- حماية المعلومات المصنفة لا تقتصر على النصوص القانونية فقط، بل تتطلب تكاملاً مع آليات تقنية كالتشفير، إدارة الهوية، والتوقيع الإلكتروني، وهي آليات لا تزال غير معتممة بالشكل المطلوب.

- فعالية الإطار القانوني تبقى مرهونة بمدى الالتزام المؤسسي والتقني بتطبيق أحكامه، وهو ما يواجه صعوبات على مستوى الإدارات العمومية.

أما فيما يتعلق بالتوصيات، فتقترح الدراسة:

- ضرورة تعزيز التكوين المستمر لموظفي الإدارات العمومية في مجال التعامل مع الوثائق المصنفة.
- تفعيل دور الهيئات الرقابية في مراقبة احترام قواعد حماية المعلومات والوثائق الإلكترونية في المؤسسات والإدارات العمومية.
- ضرورة التحديث والتطوير المستمر للمنظومة وطنية للأمن المعلوماتي سواء من الجانب القانوني أو التقني أو المؤسسي.
- مراجعة بعض النصوص القانونية لتكييفها مع التحولات السريعة في تكنولوجيا المعلومات.
- تشجيع الدراسات التطبيقية حول مدى نجاعة المنظومة القانونية في الواقع الميداني.

# قائمة المصادر والمراجع

أولاً: المصادر

1- القرآن الكريم

2- القوانين:

3. القوانين العادية:

- القانون رقم 04-15، المؤرخ في 11 ربيع الثاني عام 1436 الموافق 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر.ج.ج، العدد 06، الصادرة بتاريخ 20 ربيع الثاني عام 1436 هـ الموافق 10 فبراير سنة 2015.
- القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430 هـ الموافق لـ 5 غشت سنة 2009، يحدد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 47، الصادرة بتاريخ 25 شعبان عام 1430 هـ الموافق لـ 16 غشت سنة 2009.

4. الأوامر:

- الامر 09-21 المتعلق بحماية للمعلومات والوثائق الإدارية، المؤرخ في 9 يونيو 2021، ج.ر.ج.ج، العدد 45، المؤرخة في 9 يونيو 2021.

5. المراسيم الرئاسية:

- المرسوم الرئاسي رقم 15-261، المؤرخ في 24 ذي الحجة عام 1436 هـ الموافق لـ 8 أكتوبر سنة 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 53، الصادرة بتاريخ 24 ذي الحجة عام 1436 هـ الموافق لـ 8 أكتوبر سنة 2015 .
- المرسوم الرئاسي رقم 19-172، المؤرخ في 3 شوال عام 1440 هـ الموافق لـ 6 يونيو سنة 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، ج.ر.ج.ج، العدد 37، الصادرة بتاريخ 6 شوال عام 1440 هـ الموافق لـ 9 يونيو سنة 2019 .
- المرسوم الرئاسي رقم 20-05، المؤرخ في 24 جمادى الأولى عام 1441 هـ الموافق لـ 20 جانفي سنة 2020، يتعلق بوضع منظومة وطنية لأمن الانظمة المعلوماتية، ج.ر.ج.ج،

العدد 04، الصادرة بتاريخ أول جمادى الثانية عام 1441هـ الموافق لـ 26 جانفي سنة 2020.

- المرسوم الرئاسي رقم 20-183، المؤرخ في 21 ذو القعدة عام 1441هـ الموافق لـ 13 يوليو سنة 2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.ج.ج، العدد 40، الصادرة بتاريخ 26 ذو القعدة عام 1441هـ الموافق لـ 18 يوليو سنة 2020.

### 6. المراسيم التنفيذية:

- المرسوم التنفيذي رقم 16/142، المؤرخ في 5 ماي 2016، يحدد كفاءات حفظ الوثيقة الموقعة الكترونيا ج.ر.ج.ج، رقم 28، الصادرة في 8 ماي 2016.

### 3- المعاجم:

- أحمد محمد الشامي سيد حسب الله، المعجم الموسوعي لمصطلحات المكتبات والمعلومات (انجليزي-عربي)، دار المريح للنشر، السعودية، ط 1، 1988.

- عبد الغفور عبد الفتاح قارئ، معجم مصطلحات المكتبات والمعلومات: إنجليزي - عربي، الرياض: مكتبة الملك فهد الوطنية، السعودية، 1420هـ / 2000م.

### ثانيا: المراجع العامة

- شعبان خليفة، قاموس البنهاوي الموسوعي (عربي)، العربي للنشر والتوزيع، الرياض، السعودية، ط 1، 1990.

### ثالثا: المراجع المتخصصة

- أشرف محمد عبده، إدارة الوثائق الالكترونية، دار الجوهرة للنشر والتوزيع، القاهرة، 2015.

- ذيب بن عايض القحطاني، أمن المعلومات، مطابع مدينة الملك عبد العزيز للعلوم والتقنية، الرياض، السعودية، 2015.

- رشدي محمد علي، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الأنترنت، دار النهضة العربية للنشر والتوزيع، القاهرة، مصر، ط 1، 2000.

- عادل غزال، التسيير الإلكتروني للوثائق، دار اللمعية للنشر والتوزيع، قسنطينة، الجزائر، ط 1، 2012.

- عماد عيسى صالح محمد، المكتبات الرقمية الأسس والتطبيقات العلمية، دار المصرية اللبنانية، القاهرة، مصر، ط 1، يناير 2006.

#### رابعاً: الأطروحات والمذكرات

##### - الأطروحات:

- كحيله سارة، إدارة الوثائق الالكترونية (دراسة تقييمية لمشروع وزارة التربية الوطنية)، أطروحة مقدمة لنيل شهادة دكتوراه طور ثالث ل.م.د في علم المكتبات والتوثيق، قسم علم المكتبات والتوثيق، كلية العلوم الإنسانية، جامعة الجزائر 2، الجزائر، 2021/2020.

##### - المذكرات:

- بغداد محمد، "الأمن المعلوماتي وسبل حمايته في الجزائر -دراسة حالة مؤسسة اتصالات الجزائر -سعيدة"، مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية تخصص تسيير وإدارة المنظمات الأمنية، جامعة الدكتور مولاي الطاهر، سعيدة، 2018/2017.

- بن نعيم أسماء، دور البيئة الرقمية في تحسين خدمة الإدارة العمومية (دراسة حالة مقر ولاية المسيلة)، مذكرة ماستر، قسم علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، 2024/2023.

- زاهي كلثوم، المشاركة المعرفية في ظل البيئة الرقمية (دراسة مسحية على عينة من طلبة السنة الثانية ماستر اتصال وعلاقات عامة مستخدمى صفحة المنبر الإعلامي)، مذكرة ماستر، قسم العلوم الاجتماعية، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر، بسكرة، 2019.

- زيدان فضيلة، حماية وأمن الوثائق الإلكترونية باستخدام تطبيقات الحوسبة السحابية (دراسة على تطبيقات Google Drive وDropbox من وجهة نظر الأساتذة الجامعيين جامعة ابن خلدون تيارت أنموذجاً)، مذكرة مقدمة لنيل شهادة ماستر، قسم علم المكتبات والمعلومات، كلية العلوم الإنسانية والعلوم الاجتماعية، جامعة ابن خلدون، تيارت، الجزائر، 2024/2023.

- شارف صباح، كشرود مروى، دور الرقمنة في عصرنة الإدارة الجزائرية (قطاع العدالة نموذجاً)، مذكرة ماستر، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة تبسة، 2020/2019.

- عبد الرحمن بوكفة، الحماية القانونية للمعلومات والوثائق الإدارية، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص القانون العام، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، ام البواقي، 2023/2022.
- عبدش عبد الرحيم، بن ناصر محمد، استراتيجيات البحث المتبعة في استرجاع المعلومات في البيئة الرقمية (دراسة ميدانية مع طلبة السنة الثانية ماستر تكنولوجيا وهندسة المعلومات بجامعة عبد الحميد ابن باديس -مستغانم - أنموذجاً)، مذكرة ماستر، قسم العلوم الإنسانية، كلية العلوم الاجتماعية، جامعة عبد الحميد ابن باديس، مستغانم، 2019/2018.
- عزيزي عبد السميع، مصطفى وحال، الرقمنة وتحسين الخدمة العمومية في الجزائر، مذكرة ماستر، تخصص دولة ومؤسسات، كلية الحقوق والعلوم السياسية، جامعة يحيى فارس، المدية، 2020/2019.
- مريم ثابت، الحماية الجنائية للمعلومات والوثائق الإدارية في ظل الأمر 21-09، مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي التبسي، تبسة، 2022/2021.
- ولد شيخ خولة، بن سعدة سهام، أثر الرقمنة على فعالية الأداء داخل المؤسسة العمومية الجزائرية (دراسة حالة الملحق المحلية لوكالة التشغيل ببلدية شلالة العذارة)، مذكرة ماستر، قسم علوم الإعلام والاتصال، كلية العلوم الإنسانية والاجتماعية، جامعة يحيى فارس، المدية، 2022/2021.

#### خامسا: المقالات العلمية

- أحمد فرج احمد، الرقمنة داخل مؤسسات المعلومات ام خارجها؟ (دراسة في الاشكاليات ومعايير الاختيار)، مجلة دراسات المعلومات، جامعة الامام محمد بن سعود الإسلامية، السعودية، العدد الرابع، يناير 2009.
- بغدادى إيمان، "التوقيع الإلكتروني كبديل للتوقيع التقليدي في التجارة الإلكترونية"، مجلة الاقتصاد الدولي والعمولة، جامعة قسنطينة 1، الجزائر، المجلد 2، العدد 4، 2019.
- بوخرباش مولود، ويحة عيسى، تأثير البيئة الرقمية على مكونات الاستراتيجية التسويقية دراسة حالة موقع: Amazon.com، Revue des Réformes Economiques et Intégration، En Economie Mondiale، المدرسة العليا للتجارة، الجزائر، العدد الثاني، 2019.

- تومي يحيى، "الحماية القانونية للمعلومات والوثائق الإدارية على ضوء القانون رقم 21-09: دراسة تحليلية"، المجلة الجزائرية للحقوق والعلوم السياسية، جامعة احمد بن يحيى، تسمسيت، الجزائر، مجلد 7، عدد 2، 2022.
- حابت أمال، الجريمة المعلوماتية في التشريع الجزائري: بين قانوني 15.04 و 04.09، مجلة هيروودوت للعلوم الإنسانية والاجتماعية جامعة 8 ماي 1945، قالمة، الجزائر، المجلد 7، العدد 25، 2023.
- زاير نصيرة، عاشور حفيظة، تفعيل الرقمنة في الخدمة العمومية ودورها في تثمين الأداء الإداري، مجلة المفكر، جامعة الجزائر 2، المجلد الثامن (العدد الأول)، جوان 2024.
- فؤاد حبيب، وحنان كريبط، "أمن المعلومات ودوره في مواجهة الاعتداءات الإلكترونية على نظام معلومات المؤسسة"، مجلة المؤسسة، جامعة الجزائر 3، العدد 3، 2014.
- محمد بن فريدة، "آليات حماية المعلومات والوثائق الإدارية -دراسة من خلال أحكام الأمر 21-09"، المجلة الدولية للبحوث القانونية والسياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، المجلد 5، العدد 03، ديسمبر 2021.
- منجية بورحلة، سايجي الخامسة، منير الحمزة، التحول الرقمي ودوره في تحقيق أهداف التنمية المستدامة، مجلة الدراسات البيئية والتنمية المستدامة، جامعة الشهيد الشيخ العربي التبسي، المجلد 2، العدد الثاني، 2023.

#### سادسا: الوثائق

- سياسة تصنيف البيانات، مكتب ادارة البيانات، هيئة حقوق الانسان السعودية، الاصدار الأول، 2021.

# فهرس المحتويات

| الصفحة   | المحتويات                            |
|--|--------------------------------------|
|  | اهداء                                |
|  | شكر وتقدير                           |
|  | قائمة المختصرات                      |
| 01   | مقدمة                                |
| الفصل الأول: الإطار المفاهيمي للمعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية |                                      |
| 07   | المبحث الأول: ماهية البيئة الرقمية   |
| 07   | المطلب الأول: مفهوم الرقمنة          |
| 07   | الفرع الأول: تعريف الرقمنة           |
| 09   | الفرع الثاني: دوافع تطبيق الرقمنة    |
| 10   | الفرع الثالث: أهداف الرقمنة          |
| 10   | أولا: الأهداف الادارية               |
| 11   | ثانيا: الأهداف الاقتصادية            |
| 11   | ثالثا: الأهداف الاجتماعية            |
| 12   | المطلب الثاني: مفهوم البيئة الرقمية  |
| 12   | الفرع الأول: تعريف البيئة الرقمية    |
| 13   | الفرع الثاني: خصائص البيئة الرقمية   |
| 13   | أولا: الحداثة                        |
| 13   | ثانيا: الترابط والشبكية              |
| 14   | ثالثا: التفاعلية                     |
| 14   | رابعا: الافتراضية                    |
| 14   | الفرع الثالث: متطلبات البيئة الرقمية |
| 14   | أولا: المتطلبات البشرية المؤهلة      |
| 15   | ثانيا: المتطلبات التقنية             |
| 15   | ثالثا: متطلبات تنظيمية وقانونية      |

|  |  |
|--|--|
| 15   | رابعا: متطلبات مالية   |
| 15   | المبحث الثاني: ماهية المعلومات المصنفة والوثائق الإلكترونية                  |
| 16   | المطلب الأول: مفهوم الوثائق الإلكترونية                                      |
| 16   | الفرع الأول: تعريف الوثائق الإلكترونية                                       |
| 16   | أولا: تعريف الوثيقة  |
| 17   | ثانيا: تعريف الوثائق الإلكترونية   |
| 17   | الفرع الثاني: مكونات الوثيقة الإلكترونية                                     |
| 18   | الفرع الثالث: أنواع وأشكال الوثائق الإلكترونية                               |
| 19   | أولا: أنواع الوثائق الإلكترونية  |
| 19   | ثانيا: أشكال الوثيقة الإلكترونية   |
| 20   | الفرع الرابع: مميزات وسلبيات الوثيقة الإلكترونية                             |
| 20   | أولا: مميزات الوثيقة الإلكترونية   |
| 21   | ثانيا: سلبيات الوثائق الإلكترونية  |
| 21   | المطلب الثاني: مفهوم المعلومات المصنفة                                       |
| 22   | الفرع الأول: تعريف المعلومات المصنفة   |
| 22   | أولا: تعريف المعلومات  |
| 23   | ثانيا: تعريف المعلومات المصنفة   |
| 23   | الفرع الثاني: الخصائص والطبيعة القانونية للمعلومات                           |
| 23   | أولا: خصائص المعلومات  |
| 24   | ثانيا: الطبيعة القانونية للمعلومات   |
| 25   | الفرع الثالث: المبادئ الرئيسية لتصنيف المعلومات                              |
| 26   | الفرع الرابع: مستويات تصنيف المعلومات  |
| الفصل الثاني: آليات حماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية |  |
| 31   | المبحث الأول: الآليات الوقائية لحماية المعلومات المصنفة والوثائق الإلكترونية |
| 31   | المطلب الأول: الحماية التشريعية  |

|    |   |
|----|---|
| 31 | الفرع الأول: الأمر رقم 21-09 المتعلق بحماية المعلومات والوثائق الادارية                     |
| 31 | أولاً: تعريف بالأمر رقم 21-09 المتعلق بحماية المعلومات والوثائق الادارية                    |
| 32 | ثانياً: دوافع صدور الأمر 21-09 وسياقه   |
| 32 | ثالثاً: دور الأمر 21-09 في حماية المعلومات والوثائق   |
| 33 | الفرع الثاني: القانون رقم 15-04 الذي يحدد القواعد المتعلقة بالتوقيع والتصديق الالكترونيين   |
| 34 | أولاً: التعريف بالقانون رقم 15-04 الذي يحدد القواعد المتعلقة بالتوقيع والتصديق الالكترونيين |
| 34 | ثانياً: دوافع صدور القانون 15-04 وسياقه   |
| 35 | ثالثاً: دور القانون 15-04 في حماية الوثيقة الالكترونية                                      |
| 35 | المطلب الثاني: الآليات التقنية الداعمة للإطار القانوني                                      |
| 36 | الفرع الأول: إدارة الهوية والوصول   |
| 36 | أولاً: التحقق من الهوية   |
| 37 | ثانياً: التحكم بالوصول  |
| 38 | الفرع الثاني: التشفير   |
| 39 | الفرع الثالث: التوقيع الالكتروني  |
| 39 | المطلب الثالث: الحماية المؤسسية   |
| 40 | الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال         |
| 40 | أولاً: تشكيل الهيئة وتنظيمها  |
| 41 | ثانياً: مهام الهيئة   |
| 43 | الفرع الثاني: وكالة أمن الأنظمة المعلوماتية   |
| 43 | أولاً: تنظيم وكالة امن الأنظمة المعلوماتية وسيرها   |
| 44 | ثانياً: مهام وكالة أمن الأنظمة المعلوماتية  |
| 45 | المبحث الثاني: الآليات الجزائية لحماية المعلومات المصنفة والوثائق الإلكترونية               |
| 45 | المطلب الأول: الجرائم التقليدية الواقعة على المعلومات المصنفة والوثائق الالكترونية          |
| 45 | الفرع الأول: افشاء ونشر الوثائق والمعلومات المصنفة  |
| 46 | أولاً: جريمة افشاء المعلومات والوثائق الإدارية المصنفة                                      |

|    |   |
|----|---|
| 47 | ثانيا: جريمة افشاء الأسرار المهنية  |
| 48 | ثالثا: جريمة نشر وثائق التحقيق القضائي  |
| 48 | الفرع الثاني: الحيازة والتعدي على المعلومات والوثائق المصنفة                          |
| 48 | أولا: جنحة إخفاء الوثائق المصنفة أو اتلافها أو تزويرها                                |
| 49 | ثانيا: جريمة حيازة وثيقة مصنفة والامتناع عن تسليمها                                   |
| 49 | المطلب الثاني: الجرائم المعلوماتية الواقعة على المعلومات المصنفة والوثائق الإلكترونية |
| 49 | الفرع الأول: جريمة الدخول الغير مشروع الى الأنظمة المعلوماتية                         |
| 50 | أولا: أركان الجريمة   |
| 51 | ثانيا: العقوبات المقررة   |
| 51 | الفرع الثاني: جريمة انشاء منظومة معلوماتية بقصد نشر المعلومات والوثائق المصنفة        |
| 51 | أولا: أركان الجريمة   |
| 52 | ثانيا: العقوبات المقررة   |
| 52 | الفرع الثالث: جريمة نشر المعلومات والوثائق المصنفة بواسطة منظومة معلوماتية            |
| 52 | أولا: أركان الجريمة   |
| 53 | ثانيا: العقوبات المقررة   |
| 56 | خاتمة   |
| 59 | قائمة المصادر والمراجع  |
| 65 | فهرس المحتويات  |
| 70 | الملخص  |

الملخص:

هدفت هذه الدراسة إلى تحليل الإطار المفاهيمي والقانوني لحماية المعلومات المصنفة والوثائق الإلكترونية في البيئة الرقمية، وفي هذا السياق تناولت الدراسة في فصلها الأول تحديد المفاهيم الأساسية للمعلومات المصنفة والوثائق الإلكترونية ضمن البيئة الرقمية. بينما ركز الفصل الثاني على استعراض الآليات القانونية لحمايتها، والتي تشمل جوانب وقائية وجزائية.

وقد توصلت الدراسة إلى أن المشرع الجزائري قد بادر إلى إرساء منظومة قانونية تسعى لتوفير حماية فعالة لهذه المعلومات والوثائق من خلال الجمع بين الإجراءات الاحترازية والعقوبات الرادعة.

**الكلمات المفتاحية:** البيئة الرقمية، معلومات مصنفة، وثائق إلكترونية، حماية قانونية، أمن معلوماتي، حماية جزائية.

**Summary:**

This study aimed to analyze the conceptual and legal framework for the protection of classified information and electronic documents in the digital environment. In this context, the first chapter addressed the fundamental concepts related to classified information and electronic documents within the digital space. The second chapter focused on examining the legal mechanisms for their protection, which include both preventive and punitive aspects.

The study concluded that the Algerian legislator has undertaken to establish a legal framework intended to ensure effective protection for such information and documents, by combining precautionary measures with deterrent sanctions.

**Keywords :** Digital environment, classified information, electronic documents, legal protection, information security, penal protectio