جامعة ابن خلدون تيارت

كلية الحقوق والعلوم السياسية

قسم الحقوق

المطبوعة البداغوجية

لمقياس: تكنولوجيات الإعلام والاتصال

موجهة لطلبة السنة الأولى ماستر تخصص القانون الجنائي

من إعداد: الدكتورة المحاضرة

باهة فاطمة

السنة الجامعية:

2025-2024

جامعة ابن خلدون تيارت
المجلس العلمي
كلية الحقوق والعلوم السياسية

بسم الله الرحمن الرحيم

مقدمة

شهد العالم في العقود الأخيرة ثورة رقمية غير مسبوقة، أحدثت تحولات جذرية في بنية المجتمعات الحديثة، وامتدت تأثيراتها إلى مختلف المجالات السياسية والاقتصادية والاجتماعية.

ذلك أنّغاية المطبوعة العلمية هذه هو بناء قاعدة معرفية متينة لدى الطالب قانونية محضة بالدرجة الأولى وليست تقنية، تُمكّنه من استيعاب التداخل المتزايد بين التكنولوجيا والقانون، ومتابعة المستجدات التشريعية والتنظيمية التي تصاحب هذا التحول. فهي لا تقتصر على التوصيف النظري للتكنولوجيا، بل تسعى إلى تحليلها من منظور قانوني دقيق، وبيان آثارها الملموسة على مختلف القطاعات، وخاصة القضاء، بما يعين الطلبة على تطوير رؤى تحليلية ومنهجيات نقدية في تعاطيهم مع قضايا العصر.

ومن أهم الأهداف التي تسعى المطبوعة إلى تحقيقها كذلك، تقديم تعريف شامل ومفصّل لتكنولوجيات الإعلام والاتصال، انطلاقاً من مفاهيمها الأساسية، مروراً بوظائفها وخصائصها، وصولاً إلى بيان موقف المشرع الجزائري منها، وذلك بهدف تمكين الطلبة من فهم الخلفيات التقنية للبيئة الرقمية، باعتبار هذا الفهم شرطاً ضرورياً لأي معالجة قانونية سليمة. كما تهدف إلى تحليل الأطر القانونية الناظمة لهذه التكنولوجيات، سواء على الصعيد الوطني أو في ضوء الاتفاقيات الدولية، وهو ما يسمح للطالب بمقارنة المرجعيات القانونية، واستخلاص الفروقات والتحديات التي تعترض المواءمة التشريعية.

وتمتد أهداف المطبوعة لتشمل إبراز انعكاسات التكنولوجيات الحديثة على آليات الإثبات القانونية، المدنية منها والجنائية، من خلال دراسة أدوات مثل الكتابة الإلكترونية، التوقيع الرقمي، الأدلة الجنائية الإلكترونية، والحفظ الإلكتروني، وكل ذلك من زاوية قانونية مبنية على النصوص والممارسة القضائية. وهذا من شأنه أن يُكسب الطالب كفاءة تحليلية في التعامل مع الدليل الرقمي، وكيفية تقييمه، ومقارنته بالدليل التقليدي.

كما تسعى المطبوعة إلى تمكين الطلبة من فهم الجرائم الإلكترونية بمختلف أصنافها، من حيث المفهوم، والركائز، والتنظيم القانوني، مما يتيح لهم التميز في هذا المجال الحيوي والمطلوب في سوق العمل القانوني، خصوصاً في ظل الطلب المتزايد على مختصين قانونيين يفهمون التكنولوجيا ويتعاملون معها بمرونة وصرامة قانونية في آن.

وأخيراً، تهدف المطبوعة إلى التأكيد على أهمية التكنولوجيا كأداة فعالة لمكافحة الجريمة، وليس فقط كوسيلة لارتكابها، وذلك من خلال عرض تطبيقات الذكاء الاصطناعي في التحليل الجنائي، وأهمية نظم المراقبة والأمن السيبراني في الوقاية من الجريمة، مع الوقوف على الإطار القانوني المنظم لذلك.

إن هذه الأهداف مجتمعة لا تسعى فقط إلى تثقيف الطالب، وإنما إلى تأهيله ليكون فاعلًا قانونيًا مستقبليًا قادراً على الإسهام في تطوير الممارسة القانونية والقضائية في الجزائر، بما يتماشى مع متطلبات العصر الرقمي ومقتضيات العدالة المعاصرة.

ولتحقيق هذه الأهداف من المطبوعة ارتأينا تقسيمها الى اربعة فصول:

حيث يتناول الفصل الأول :الإطار المفاهيمي لتكنولوجيات الإعلام والاتصال، ويركّز على بناء الخلفية النظرية والمعرفية التي تمكّن القارئ من استيعاب طبيعة هذه التكنولوجيات وتطورها. في هذا الإطار، يتناول المبحث الأول ماهية هذه التكنولوجيات من خلال تحديد المفاهيم المختلفة المرتبطة بها، كتعريفات التكنولوجيا، وتكنولوجيا الإعلام، وتكنولوجيا الاتصال، وصولاً إلى

وقد كانت تكنولوجيات الإعلام والاتصال في قلب هذه الثورة، إذ ساهمت في إحداث طفرة نوعية في كيفية التواصل، وتبادل المعلومات، وتسيير المعاملات. وفي الجزائر، كما في باقي دول العالم، أصبحت هذه التكنولوجيات أداة محورية في تحديث الإدارة والخدمات، وتعزيز الشفافية والكفاءة، نظراً لما توفره من سرعة ودقة وفعالية في الأداء.

غير أن هذا التحول التكنولوجي لم يخلُ من تحديات قانونية ومجتمعية معقدة، إذ ظهرت ممارسات مستحدثة لم يكن لها وجود في البيئة التقليدية، مثل الجرائم الإلكترونية، وانتهاك الخصوصية الرقمية، وصعوبة ضبط الأدلة الإلكترونية. وهو ما فرض على المشرعين ضرورة إعادة النظر في التشريعات القائمة، وتكييفها مع هذه المعطيات الجديدة، سعياً لتحقيق توازن بين استغلال الإمكانات الهائلة التي توفرها التكنولوجيا من جهة، وضمان حماية الحقوق والحريات من جهة أخرى، في ظل تصاعد المخاطر المرتبطة باستخدامها غير المشروع.

وفي هذا السياق، تبرز أهمية التكوين القانوني المتخصص، خاصة بالنسبة لطلبة ماستر العلوم الجنائية، الذين أصبح لزاماً عليهم استيعاب الأبعاد القانونية لتكنولوجيات الإعلام والاتصال، ليس فقط من خلال معرفة المفاهيم العامة، بل أيضاً من خلال التمكن من أدوات الإثبات الحديثة، وفهم طبيعة الجريمة الرقمية وآليات مكافحتها. من هنا جاءت هذه المطبوعة كأداة أكاديمية تحليلية شاملة، تهدف إلى تزويد الطلبة برؤية منهجية متكاملة تجمع بين الأساس النظري والتطبيقات الواقعية، بما يمكّنهم من التعامل بفعالية مع الإشكالات القانونية المستحدثة في الفضاء الرقمي.

تكتسي دراسة تكنولوجيات الإعلام والاتصال وانعكاساتها القانونية أهمية متزايدة في ظل التحوّل الرقمي العميق الذي طال مختلف مناحي الحياة، وأثر بشكل مباشر في المنظومة القانونية والعدلية. فقد أصبحت هذه التكنولوجيات مكوّناً أساسياً في تسيير العلاقات والتعاملات، لما توفره من إمكانات هائلة في تخزين المعطيات، ومعالجتها، وتبادلها بسرعة ودقة. ونتيجة لذلك، تغيّرت طبيعة العلاقات القانونية، وأساليب الإثبات، بل وحتى أنماط ارتكاب الجرائم. وفي هذا الإطار، أضحى من الضروري على القانونيين فهم البيئة الرقمية، لا كمجرد خلفية تقنية، بل كمجال قانوني يتطلب قراءة جديدة للأدوات والضوابط المعتمدة في ممارسات العدالة.

ومع تصاعد وتيرة الرقمنة في الجزائر، وما يرافقها من مشاريع لرقمنة الخدمات العمومية والعدلية، برزت تحديات تشريعية ومؤسساتية تتعلق بكيفية تنظيم هذه العمليات وضمان مشروعيتها، دون المساس بحقوق الأفراد. فقد أفرزت البيئة الرقمية جرائم إلكترونية مستحدثة، معقّدة، وعابرة للحدود، يصعب إثباتها بوسائل تقليدية، الأمر الذي يفرض على رجل القانون، لاسيما في الميدان الجنائي، أن يكون متمكناً من أدوات القانون الرقمي، وقادراً على التفاعل مع القضايا التقنية بمنهجية قانونية دقيقة. من هنا تنبع أهمية تضمين هذه المحاور في المقررات الدراسية، وتأهيل الطلبة لتجاوز الفجوة التقليدية بين القانون والتكنولوجيا.

وتهدف هذه المطبوعة، انطلاقاً من طبيعتها التعليمية، إلى سد فراغ بيداغوجي حقيقي من خلال تقديم إطار أكاديمي متكامل يُواكب المستجدات الرقمية ذات الصلة بالمجال القانوني، ويتيح لطلبة ماستر العلوم الجنائية اكتساب رؤية واضحة حول الأبعاد القانونية لتكنولوجيات الإعلام والاتصال. ورغم أن المقياس يحمل عنوان "تكنولوجيات الإعلام والاتصال" دون الإشارة الصريحة إلى انعكاساتها القانونية، إلا أن طبيعة التكوين القانوني الذي ينتمي إليه الطلبة تفرض التطرق إلى هذه الأبعاد، ولو لم تكن مسطرة ضمن الكانفا المقررة للمقياس.

وقد كانت تكنولوجيات الإعلام والاتصال في قلب هذه الثورة، إذ ساهمت في إحداث طفرة نوعية في كيفية التواصل، وتبادل المعلومات، وتسيير المعاملات. وفي الجزائر، كما في باقي دول العالم، أصبحت هذه التكنولوجيات أداة محورية في تحديث الإدارة والخدمات، وتعزيز الشفافية والكفاءة، نظراً لما توفره من سرعة ودقة وفعالية في الأداء.

غير أن هذا التحول التكنولوجي لم يخلُ من تحديات قانونية ومجتمعية معقدة، إذ ظهرت ممارسات مستحدثة لم يكن لها وجود في البيئة التقليدية، مثل الجرائم الإلكترونية، وانتهاك الخصوصية الرقمية، وصعوبة ضبط الأدلة الإلكترونية. وهو ما فرض على المشرعين ضرورة إعادة النظر في التشريعات القائمة، وتكييفها مع هذه المعطيات الجديدة، سعياً لتحقيق توازن بين استغلال الإمكانات الهائلة التي توفرها التكنولوجيا من جهة، وضمان حماية الحقوق والحريات من جهة أخرى، في ظل تصاعد المخاطر المرتبطة باستخدامها غير المشروع.

وفي هذا السياق، تبرز أهمية التكوين القانوني المتخصص، خاصة بالنسبة لطلبة ماستر العلوم الجنائية، الذين أصبح لزاماً عليهم استيعاب الأبعاد القانونية لتكنولوجيات الإعلام والاتصال، ليس فقط من خلال معرفة المفاهيم العامة، بل أيضاً من خلال التمكن من أدوات الإثبات الحديثة، وفهم طبيعة الجريمة الرقمية وآليات مكافحتها. من هنا جاءت هذه المطبوعة كأداة أكاديمية تحليلية شاملة، تهدف إلى تزويد الطلبة برؤية منهجية متكاملة تجمع بين الأساس النظري والتطبيقات الواقعية، بما يمكّنهم من التعامل بفعالية مع الإشكالات القانونية المستحدثة في الفضاء الرقمي.

تكتسي دراسة تكنولوجيات الإعلام والاتصال وانعكاساتها القانونية أهمية متزايدة في ظل التحوّل الرقمي العميق الذي طال مختلف مناحي الحياة، وأثر بشكل مباشر في المنظومة القانونية والعدلية. فقد أصبحت هذه التكنولوجيات مكوّناً أساسياً في تسيير العلاقات والتعاملات، لما توفره من إمكانات هائلة في تخزين المعطيات، ومعالجتها، وتبادلها بسرعة ودقة. ونتيجة لذلك، تغيّرت طبيعة العلاقات القانونية، وأساليب الإثبات، بل وحتى أنماط ارتكاب الجرائم. وفي هذا الإطار، أضحى من الضروري على القانونيين فهم البيئة الرقمية، لا كمجرد خلفية تقنية، بل كمجال قانوني يتطلب قراءة جديدة للأدوات والضوابط المعتمدة في ممارسات العدالة.

ومع تصاعد وتيرة الرقمنة في الجزائر، وما يرافقها من مشاريع لرقمنة الخدمات العمومية والعدلية، برزت تحديات تشريعية ومؤسساتية تتعلق بكيفية تنظيم هذه العمليات وضمان مشروعيتها، دون المساس بحقوق الأفراد. فقد أفرزت البيئة الرقمية جرائم إلكترونية مستحدثة، معقّدة، وعابرة للحدود، يصعب إثباتها بوسائل تقليدية، الأمر الذي يفرض على رجل القانون، لاسيما في الميدان الجنائي، أن يكون متمكناً من أدوات القانون الرقمي، وقادراً على التفاعل مع القضايا التقنية بمنهجية قانونية دقيقة. من هنا تنبع أهمية تضمين هذه المحاور في المقررات الدراسية، وتأهيل الطلبة لتجاوز الفجوة التقليدية بين القانون والتكنولوجيا.

وتهدف هذه المطبوعة، انطلاقاً من طبيعتها التعليمية، إلى سد فراغ بيداغوجي حقيقي من خلال تقديم إطار أكاديمي متكامل يُواكب المستجدات الرقمية ذات الصلة بالمجال القانوني، ويتيح لطلبة ماستر العلوم الجنائية اكتساب رؤية واضحة حول الأبعاد القانونية لتكنولوجيات الإعلام والاتصال. ورغم أن المقياس يحمل عنوان "تكنولوجيات الإعلام والاتصال" دون الإشارة الصريحة إلى انعكاساتها القانونية، إلا أن طبيعة التكوين القانوني الذي ينتمي إليه الطلبة تفرض التطرق إلى هذه الأبعاد، ولو لم تكن مسطرة ضمن الكانفا المقررة للمقياس.

ذلك أنّغاية المطبوعة العلمية هذه هو بناء قاعدة معرفية متينة لدى الطالب قانونية محضة بالدرجة الأولى وليست تقنية، تُمكّنه من استيعاب التداخل المتزايد بين التكنولوجيا والقانون، ومتابعة المستجدات التشريعية والتنظيمية التي تصاحب هذا التحول. فهي لا تقتصر على التوصيف النظري للتكنولوجيا، بل تسعى إلى تحليلها من منظور قانوني دقيق، وبيان آثارها الملموسة على مختلف القطاعات، وخاصة القضاء، بما يعين الطلبة على تطوير رؤى تحليلية ومنهجيات نقدية في تعاطيهم مع قضايا العصر.

ومن أهم الأهداف التي تسعى المطبوعة إلى تحقيقها كذلك، تقديم تعريف شامل ومفصّل لتكنولوجيات الإعلام والاتصال، انطلاقاً من مفاهيمها الأساسية، مروراً بوظائفها وخصائصها، وصولاً إلى بيان موقف المشرع الجزائري منها، وذلك بهدف تمكين الطلبة من فهم الخلفيات التقنية للبيئة الرقمية، باعتبار هذا الفهم شرطاً ضرورياً لأي معالجة قانونية سليمة. كما تهدف إلى تحليل الأطر القانونية الناظمة لهذه التكنولوجيات، سواء على الصعيد الوطني أو في ضوء الاتفاقيات الدولية، وهو ما يسمح للطالب بمقارنة المرجعيات القانونية، واستخلاص الفروقات والتحديات التي تعترض المواءمة التشريعية.

وتمتد أهداف المطبوعة لتشمل إبراز انعكاسات التكنولوجيات الحديثة على آليات الإثبات القانونية، المدنية منها والجنائية، من خلال دراسة أدوات مثل الكتابة الإلكترونية، التوقيع الرقمي، الأدلة الجنائية الإلكترونية، والحفظ الإلكتروني، وكل ذلك من زاوية قانونية مبنية على النصوص والممارسة القضائية. وهذا من شأنه أن يُكسب الطالب كفاءة تحليلية في التعامل مع الدليل الرقمي، وكيفية تقييمه، ومقارنته بالدليل التقليدي.

كما تسعى المطبوعة إلى تمكين الطلبة من فهم الجرائم الإلكترونية بمختلف أصنافها، من حيث المفهوم، والركائز، والتنظيم القانوني، مما يتيح لهم التميز في هذا المجال الحيوي والمطلوب في سوق العمل القانوني، خصوصاً في ظل الطلب المتزايد على مختصين قانونيين يفهمون التكنولوجيا ويتعاملون معها بمرونة وصرامة قانونية في آن.

وأخيراً، تهدف المطبوعة إلى التأكيد على أهمية التكنولوجيا كأداة فعالة لمكافحة الجريمة، وليس فقط كوسيلة لارتكابها، وذلك من خلال عرض تطبيقات الذكاء الاصطناعي في التحليل الجنائي، وأهمية نظم المراقبة والأمن السيبراني في الوقاية من الجريمة، مع الوقوف على الإطار القانوني المنظم لذلك.

إن هذه الأهداف مجتمعة لا تسعى فقط إلى تثقيف الطالب، وإنما إلى تأهيله ليكون فاعلًا قانونيًا مستقبليًا قادراً على الإسهام في تطوير الممارسة القانونية والقضائية في الجزائر، بما يتماشى مع متطلبات العصر الرقمي ومقتضيات العدالة المعاصرة.

ولتحقيق هذه الأهداف من المطبوعة ارتأينا تقسيمها الى اربعة فصول:

حيث يتناول الفصل الأول :الإطار المفاهيمي لتكنولوجيات الإعلام والاتصال، ويركّز على بناء الخلفية النظرية والمعرفية التي تمكّن القارئ من استيعاب طبيعة هذه التكنولوجيات وتطورها. في هذا الإطار، يتناول المبحث الأول ماهية هذه التكنولوجيات من خلال تحديد المفاهيم المختلفة المرتبطة بها، كتعريفات التكنولوجيا، وتكنولوجيا الإعلام، وتكنولوجيا الاتصال، وصولاً إلى

المفهوم الشامل لتكنولوجيات الإعلام والاتصال، مع التوقف عند موقف المشرع الجزائري منها. ثم يتناول خصائص هذه التكنولوجيات ووظائفها الحيوية في العصر الرقمي، لينتقل بعد ذلك إلى عرض للتطور التاريخي الذي شهدته، من البدايات الأولى للتقنيات السمعية والبصرية إلى غاية ظهور الثورة الرقمية. أما المبحث الثاني، فيُعنى بالثورة الرقمية وانعكاساتها القانونية، حيث يتم التطرق إلى الأبعاد القانونية للتحول الرقمي، وتأثيره على حماية الحقوق الأساسية، لاسيما في ما يتعلق بسرية البيانات، والعقود الرقمية، والجرائم الإلكترونية، والذكاء الاصطناعي، مع تحليل الإطار القانوني الوطني والدولي الذي يسعى لتنظيم هذه التحولات.

أما الفصل الثاني، فهو يُركّز على العلاقة بين تكنولوجيات الإعلام والاتصال ورقمنة الخدمات، حيث يستعرض، في المبحث الأول، مفهوم رقمنة الخدمات من منظور قانوني وإداري، ويبحث في أهدافها الاستراتيجية، وأهميتها في تطوير الأداء المؤسساتي وتحسين العلاقة بين المواطن والإدارة، لاسيما في السياق الجزائري الذي يشهد جهوداً متزايدة للتحول الرقمي. ثم ينتقل إلى المبحث الثاني الذي يعالج واقع الرقمنة في القطاعات الحيوية في الجزائر، كالحالة المدنية، والعدالة، والبريد، والتعليم العالي، والضمان الاجتماعي، ويستعرض التحديات والعراقيل التي تعترض هذا التحول، إلى جانب تحديد المتطلبات الأساسية التي ينبغي توفرها لضمان نجاح الرقمنة، سواء على مستوى التشريعات، أو البنية التحتية، أو الكفاءات البشرية.

والفصل الثالث يتناول الدور المتنامي لتكنولوجيات الإعلام والاتصال في المجال القانوني والقضائي، من خلال التركيز على التأثيرات المباشرة لهذه التكنولوجيات على نظام الإثبات. يتناول المبحث الأول أثرها في الإثبات المدني والجنائي، عبر دراسة الوسائل التقنية المستحدثة، مثل الكتابة الإلكترونية، والتوقيع الإلكتروني، والدليل الرقمي، وشروط قبولها أمام القضاء، مع بيان موقف المشرع الجزائري. أما المبحث الثاني، فيتناول دور هذه التكنولوجيات في تأمين الأدلة القانونية من خلال نظامي التصديق والحفظ الإلكترونيين، حيث يتم تحليل البنية القانونية والتنظيمية لمؤدي خدمات التصديق والحفظ، والشروط القانونية المقررة لممارسة هذه المهام الحيوية، بما يضمن سلامة المعاملات الإلكترونية ويعزز من حجيتها أمام الجهات القضائية.

وفي الفصل الرابع، تُختم المطبوعة بمعالجة العلاقة الجدلية بين تكنولوجيات الإعلام والاتصال والجريمة الإلكترونية، حيث يتم في المبحث الأول تحليل الجريمة الإلكترونية كظاهرة مستحدثة في ظل التطور التكنولوجي، من حيث المفهوم، والخصائص، وأنواع الجرائم المرتكبة، مع تقديم عرض مفصل للإطار القانوني الجزائري الذي يُعنى بمكافحتها سواء في قانون العقوبات أو القوانين الخاصة. أما المبحث الثاني، فيُبرز الوجه الآخر للتكنولوجيا، أي باعتبارها وسيلة فعّالة لمكافحة الجريمة، سواء من خلال توظيفها في عمليات التحقيق والتحليل الجنائي، أو في الوقاية الاستباقية عبر أنظمة الذكاء الاصطناعي، والتشفير، والأمن السيبراني، مع التركيز على الضوابط القانونية التي تحكم هذا الاستخدام لضمان التوازن بين الفعالية الأمنية وحماية الحقوق الفردية.

وترتكز هذه المطبوعة على المنهج التحليلي والمقارن، وتستند إلى جملة من النصوص القانونية الوطنية والدولية، والوثائق المرجعية الرسمية، إلى جانب آراء الفقهاء والاجتهادات القضائية ذات الصلة. وحرصاً على الفائدة البيداغوجية، تم اعتماد لغة واضحة وأمثلة تطبيقية من الواقع القانوني الجزائري.

لا شك أن موضوع هذه المطبوعة يُعد من أكثر المواضيع المعاصرة أهمية، حيث يفرض على طلبة الماستر، وبخاصة في تخصص العلوم الجنائية، الإلمام بالجوانب التقنية للتكنولوجيا الحديثة، وفهم الانعكاسات القانونية والاجتماعية المرتبطة بها. فالفاعل القانوني اليوم، سواء كان قاضياً أو محامياً أو باحثاً، مدعو إلى فهم معمق للتحولات الرقمية، بما يتيح له مواكبة العصر، والمساهمة في تطوير تشريعات تتسم بالفعالية والمرونة.

وختاماً، نأمل أن تشكل هذه المطبوعة مرجعاً علمياً وأداةً تعليمية فاعلة للطلبة، وأن تسهم في إثراء النقاش الأكاديمي والبحثي حول العلاقة المعقدة بين القانون والتكنولوجيا، وفي بناء وعي قانوني رقمي يستجيب لتحديات الزمن المعاصر.

الفصل الأول: الاطار المفاهيمي لتكنولوجيات الإعلام والاتصال

شهد العالم في العقود الأخيرة تطورات متسارعة في مجال تكنولوجيات الإعلام والاتصال، مما أدى إلى إحداث تحولات جذرية في كيفية تبادل المعلومات وإدارة المعرفة. وقد أصبحت هذه التكنولوجيات من العوامل الأساسية في تطوير مختلف القطاعات الاقتصادية والاجتماعية والسياسية، حيث ساهمت في تسهيل عمليات الاتصال وتعزيز التدفق الحر للمعلومات على المستويين المحلي والدولي.

يركز هذا الفصل على الإطار العام لتكنولوجيات الإعلام والاتصال من خلال تناول مفهومها وتطورها التاريخي، مع تسليط الضوء على خصائصها ووظائفها المختلفة، إضافة إلى علاقتها بالتحولات القانونية التي أفرزتها الثورة الرقمية. كما يتناول البنية التحتية الرقمية ودورها المحوري في الاتصال، متتبعًا مراحل تطور شبكات الاتصال السلكية واللاسلكية، وأثر الإنترنت والذكاء الاصطناعي في هذا المجال، فضلًا عن أهمية الأقمار الصناعية في دعم منظومة الاتصالات الحديثة. وفي سياق آخر، يناقش هذا الفصل الأبعاد القانونية للثورة الرقمية، من خلال تحليل انعكاسات التطور التكنولوجي على حقوق الإنسان، وتسليط الضوء على التحديات المرتبطة بسرية البيانات، فضلًا عن دراسة الإطار التشريعي الدولي والوطني الذي ينظم هذا القطاع، مع التركيز على التشريعات الجزائرية الخاصة بتكنولوجيات الاعلام والاتصال وابعادها القانونية.

المبحث الأول: ماهية تكنولوجيات الإعلام والاتصال

أدى التطور التكنولوجي إلى بروز تكنولوجيات الإعلام والاتصال كعامل رئيسي في دعم المجتمعات الحديثة، حيث لم تعد وسائل الاتصال التقليدية كافية لمواكبة التغيرات المتسارعة في

نقل المعلومات وتخزينها وتحليلها. وباتت هذه التكنولوجيات تساهم بشكل كبير في بناء مجتمعات المعرفة وتعزيز الاقتصاد الرقمي، ما دفع العديد من الدول إلى تطوير سياسات وتشريعات تتلاءم مع هذه التحولات.

يهدف هذا المبحث إلى تقديم تصور واضح لمفهوم تكنولوجيات الإعلام والاتصال، عبر استعراض تطورها التاريخي وأبرز المحطات التي شهدها هذا المجال. كما يتناول خصائص هذه التكنولوجيات ووظائفها التي جعلتها أداة رئيسية في التفاعل الاجتماعي والاقتصادي والسياسي. وأخيرًا، يناقش العلاقة بين تكنولوجيات الإعلام والاتصال والتحولات القانونية، خاصة في ظل التحديات التي يفرضها الاستخدام الواسع للوسائط الرقمية وضرورة وجود أطر قانونية تضمن الاستخدام المسؤول لهذه التقنيات.

المطلب الأول :مفهوم تكنولوجيات الإعلام والاتصال (ICT)

شهد العالم في العقود الأخيرة تطورًا غير مسبوق في مجال التكنولوجيا، مما انعكس بشكل مباشر على طرق معالجة المعلومات ونقلها وتخزينها. وقد أدى هذا التطور إلى بروز مفاهيم متعددة، منها تكنولوجيا المعلومات وتكنولوجيا الإعلام وتكنولوجيا الاتصال، والتي أصبحت تشكل الأساس الذي يقوم عليه المجتمع الرقمي المعاصر.

في هذا الإطار، يسعى هذا المطلب إلى تحديد مفهوم التكنولوجيا بصفة عامة، ثم التطرق إلى مفهوم تكنولوجيا المعلومات باعتبارها الإطار الأشمل الذي يندرج ضمنه كل من تكنولوجيا الإعلام والاتصال. كما سيتم التمييز بين تكنولوجيا الإعلام، التي تركز على إنتاج ونشر المحتوى الإعلامي، وتكنولوجيا الاتصال، التي تهتم بوسائل نقل المعلومات والتفاعل بين الأفراد والمؤسسات. وأخيرًا، سيتم تقديم خلاصة شاملة لمفهوم تكنولوجيات الإعلام والاتصال، بما يبرز تكاملها وأهميتها في العصر الرقمي. كما ستعمد الدراسة الى تحديد موقف المشرع الجزائري من تعريف تكنولوجيات الاعلام والاتصال في القانون الجزائري المنظم لها.

أولا: تعريف التكنولوجيا

التكنولوجيا عبارة عن مجموعة من الاختراعات والتقنيات التي تسهم في تسهيل حياة الإنسان اليومية. وعلى الرغم من انتشار استخدامها في العصر الحديث، فإن أصولها تمتد إلى بدايات البشرية، حيث كان كل تطور أو ابتكار بشري وسيلة لتحسين الأداء وزيادة كفاءة تنفيذ المهام. ويعود أصل مصطلح "تكنولوجيا" إلى اللغة اليونانية، حيث يتألف من جزأين: **"Techno"** وتعني المهارة أو الحرفة أو الفن. **"Logie"**وتعني العلم أو الدراسة. ولهذا يسمى المفهوم كاملا لدى الكثير من الكتاب والباحثين تقانه المعلومات رغبه منهم في تعريب المصطلح اذا تستخدم اللغه العربيه مصطلح تقنه او اتقن وتعني احكام الامر اما التقانه فهي صفه الامر المحكم الصنع وسنعتمد المصطلحين على حد السواء وعرفت ايضا بانها علم الفنون الصناعيه كما ان التكنولوجيا هي طريقه فنيه لتحقيق غرض عملي او هي الوسائل المستخدمه لتوافر كل ما هو ضروري لمعيشه الناس ورفاهيتهم

ويمكن تعريف التكنولوجيا على أنها "علم الأداء أو التطبيق"، فهي تشمل مجموعة من الفنون والمهارات المستخدمة في الابتكار والإنتاج. وقد برز هذا المصطلح بشكل واضح خلال الثورة الصناعية، حيث أصبحت الآلة عنصرًا أساسيًا في عمليات الإنتاج الصناعي.

واصطلاحيا عرفت التكنولوجيا بتعريفات كثيره نريد بعضها فهي كما راها البعض تشير الى المهارات والمعرفه والخبره وهيئه المعرفه العلميه والادوات والمكائن والمعد المعدات التي تستعمل في التصميم والانتاج والتوزيع او انها عمليه تحويل المواد الاوليه الى منتجات وخدمات جاهزه من خلال الطرائق والاساليب والادوات والمعدات وكل ما له علاقه بهذا التحويل. وبمعنى ابسط فان التكنولوجيا تعني محاوله تطويع القوى لمصلحته وخدمه البشر[1].

كما يُنظر إلى التكنولوجيا وفق ثلاثة مفاهيم رئيسية:

1. **التكنولوجيا كعملية :**وهي التطبيق المنهجي للمعرفة العلمية بهدف تحقيق غرض محدد يؤدي إلى تحقيق هدف معين.
2. **التكنولوجيا كمنتج :**وهي المخرجات الفعلية لتطبيق المعرفة العلمية، مثل إنتاج الآلات والمعدات.
3. **التكنولوجيا كمزيج بين الأسلوب والمنتج :**وهو المفهوم الذي يؤكد على التلازم بين عملية الاختراع وعملية الإنتاج، بحيث لا يمكن فصل التكنولوجيا كأسلوب تطبيقي عن التكنولوجيا كمنتج.

ومن الأمثلة الواضحة على ذلك **الحاسب الآلي**، الذي يشهد تطورًا مستمرًا سواء في تصميمه أو في البرمجيات المصاحبة له، مما يؤدي إلى توسيع وظائفه وإمكاناته.

ويمكن تعريف التكنولوجيا في جانبها الاجرائي بأنها تلك الأدوات والوسائل والابتكارات التي توصل إليها الانسان في ميدان الإعلام والاتصال نتيجة العديد من العوامل اجتماعية نفسية سياسية اقتصادية...، وتتسم هذه التكنولوجيا بالتطور السريع والمرونة والاندماج والتفاعلية وكل هذا يصب في مصلحة الانسان[2].

كما ان هناك فرق بين التكنولوجيا والتقنية: ذلك أنّ التقنية :(Technique) تعني الأسلوب أو الطريقة المستخدمة في التعامل مع الأدوات والوسائل، وتشمل استخدام الموارد المتاحة أو توظيف المعرفة أو تنفيذ حركات يدوية لتحقيق مهام معينة. أما التكنولوجيا :(Technology) تشمل التقنيات المختلفة ولكنها تتجاوز ذلك لتشمل تطوير الأدوات والوسائل ذاتها، بالإضافة إلى التطبيقات العملية للمعرفة العلمية.

وبالتالي، يمكن اعتبار التقنية جزءًا من التكنولوجيا، حيث أن التكنولوجيا تتعلق بعملية التطوير والابتكار، في حين أن التقنية تُركز على كيفية الاستخدام الفعّال للأدوات والوسائل المتاحة.

---

[1] - حيدر شاكر البرزنجي، محمود حسن جمعة ، تكنولوجيا ونظم المعلومات في المنظمات المعاصرة، منظور اداري تكنولوجي، 2013، ص 17.

[2] - ابراهيم عمر يحياوي، تأثير تكنولوجيا الاعلام والاتصال على العملية التعليمية في الجزائر، دار اليازوزي ، 2019، ص 29.

ثانيا: تعريف تكنولوجيا المعلومات :

المعلومات مصطلح مشتق من الكلمة اللاتينية "إنفورمانيو"، والتي تعني الإبلاغ أو تقديم صورة يمكن للعقل استيعابها. لغويًا، يُقصد بالمعلومات أي حقيقة أو معلومة مفيدة، أما اصطلاحًا، فهي مجموعة من البيانات المنظمة والمترابطة حول موضوع معين، وتشمل حقائق ومفاهيم وآراء واستنتاجات ومعتقدات تسهم في تكوين المعرفة والخبرة المحسوسة ذات قيمة يمكن إدراكها سواء في الاستخدام الحالي أو المستقبلي.

تُستخلص المعلومات من خلال معالجة البيانات عبر عمليات التبويب والتصنيف والتحليل والتنظيم بطريقة تحقق هدفًا محددًا. ورغم تعدد التعريفات الخاصة بالمعلومات، إلا أن التعريف الأكثر شمولًا في مجال نظم المعلومات هو أن المعلومات عبارة عن بيانات تمت معالجتها وإعدادها لتصبح أكثر فائدة، مما يعزز قيمتها في الاستخدام الراهن أو المتوقع مستقبلاً[3].

عرفتها منظمه اليونسكو 2005 بانها مجموعه المعرفه العلميه والتكنولوجيه والهندسيه والاساليب الاداريه المستخدمه في تداول ومعالجه المعلومات كما هناك من عرفها بانها جميع تقنيات المتطوره التي تستخدم في تحويل البيانات بمختلف اشكالها الى معلومات بمختلف انواعها والتي تفيد المستخدمين لها في مجالات الحياه كافه. كما عرفتها الامم المتحده انها الوسائل الالكترونيه التي تقوم بمعالجه وتوصيل المعلومات التي توفر او تدعم الانشطه الاقتصاديه وتطبيقاتها باستخدام اجهزه الكمبيوتر والبرمجيات والاتصالات السلكيه واللاسلكيه والصناعات القائمه الكترونيا لذلك فكثيرا ما يرتبط لفظ اتصالات بالمعلومات وتعرف بانها تكنولوجيا المعلومات والاتصالات[4].

وعليه يمكن أن يضمن مفهوم تكنوولجيا العلومات مفهومين احدها مادي وآخر معنوي: فالمفهوم المادي : لتكنولوجيا المعلومات هي عبارة عن كل تلك التجهيزات والمعدات وبرامج الكمبيوتر التي تسمح لنا بحفظ المعلومات وتخزينها وتنظيمها واسترجاعها وعرضها والتعديل عليها وغير ذلك كالماسحات الضوئية والحواسيب والوسائط الالكترونية بمختلف انواعها والمفهوم المعنوي يعبر عن العمليات التي نقوم بها على تلك التجهيزات والمعدات فهي ادخال او تطبيق الدوات التقنية المتصلة بعلم الادارة

وعلى أساس ما تقدم فإنّ تكنولوجيا المعلومات هي الاستخدام والاستثمار المفيد والمثل مختلف أنواع المعارف، والبحث عن افضل الوسائل والسبل التي تسهل الحصول على المعلومات، والتي تقودنا إلى المعرفة، وهي عمليات التخزين والحفظ والتحليل والنقل والبث للمعلومات الالكترونية في جميع أشكالها وتطبيقها والتي تتم بواسطة الحاسوب الالكتروني والاتصالات السلكية واللاسلكية وتعمل على اساس الالكترونيات الدقيقة ، وجعها متاحة لمستفيدين منها وتبادلها[5].

---

[3] - حيدر شاكر البرزنجي، محمود حسن جمعة ، المرجع السابق، ص 17.

[4] - منال العشري تكنولوجيا المعلومات وراس المال البشري رؤيه للتنميه المستدامه 2030 دار التعليم الجامعي الاسكندريه، ص 34.

[5] - عامر ابراهيم قنديلجي، إيمان فاضل السامراني، تكنولوجيا المعلومات وتطبيقاتها، الطبعة الولى ، 2009، الوراق للنشر والتوزيع، ص 40.

ثالثا: تعريف تكنولوجيا الاعلام

الإعلام في اللغة مشتق من الفعل "أَعْلَمَ"، أي أَخْبَرَ وأوصل المعلومة إلى الغير، والمصدر (*إعلاماً*) . ومعنى (*أعلم*) : قام بالتعريف *والإخبار*[6] ويعني إيصال الخبر أو نقل المعرفة من طرف إلى آخر. ويرتبط الإعلام بالتبليغ والإخبار، حيث يكون الهدف منه جعل المتلقي على دراية بمحتوى معين، سواء كان ذلك شفهيًا أو كتابيًا أو عبر وسائل أخرى.

أما في الاصطلاح، فالإعلام يُعرّف على أنه العملية التي يتم من خلالها نقل المعلومات أو الأخبار أو الأفكار إلى الجمهور عبر وسائل مختلفة، سواء كانت وسائل تقليدية كالصحف والإذاعة والتلفزيون، أو حديثة كوسائل التواصل الرقمي والإنترنت. ويهدف الإعلام إلى توعية الأفراد، وتزويدهم بالمعلومات التي تساعدهم على فهم الأحداث والقضايا، كما يسهم في تشكيل الرأي العام والتأثير في المجتمع.

من ناحية أخرى، تُشير كلمة "إعلام" في جوهرها إلى الإخبار وتقديم المعلومات. وعملية نقل الأخبار والمعلومات تستلزم وجود رسالة إعلامية تحتوي على محتوى محدد، مثل الأخبار أو المعلومات أو الآراء والأفكار، التي تنتقل من المرسل إلى المستقبل في اتجاه واحد.

أما على مستوى الدول أو الأنظمة السياسية، فإن الإعلام يُعد وسيلة لتعريف الجمهور بقضايا العصر والتحديات التي تواجه المجتمع، إلى جانب توضيح كيفية التعامل مع هذه القضايا وفق الأسس والمبادئ التي يعتمدها النظام السياسي للدولة. ويتم ذلك من خلال مختلف وسائل الإعلام المتاحة التي تُعد أدوات فعالة في نقل الرسائل والتأثير على الرأي العام[7].

وبناءً على ذلك، يمكن تعريف الإعلام بأنه عملية نقل المعلومات والمعارف والثقافات الفكرية والسلوكية بوسائل وأدوات إعلامية واتصالية متنوعة، تهدف إلى التأثير في الفكر والمعتقدات وسلوكيات الأفراد داخل المجتمع.

وتُشير تكنولوجيا الإعلام إلى مجموعة الأدوات والوسائل التقنية المستخدمة في جمع الأخبار والمعلومات والصور والحقائق والرسائل والاراء ... وتخزينها ومعالجتها، ونقلها، وبثها إلى الجمهور. حتى يكونو على دراية بها والوصول إلى وضع يمكنهم من اتخاذ القرارات السليمة. وتشمل هذه التكنولوجيا الأجهزة المادية، مثل الكاميرات وأجهزة البث، إلى جانب البرمجيات المتطورة التي تعزز عمليات الإنتاج الإعلامي. ومع التطور الرقمي، أصبح للإعلام بُعد جديد قائم على الذكاء الاصطناعي، وتحليل البيانات الضخمة، مما أدى إلى تحسين سرعة ودقة نشر المعلومات.

رابعا: تعريف تكنولوجيا الاتصال:

جاء في *لسان العرب* لابن منظور أن "الاتصال" و"الوَصْلة" يشيران إلى ما اتّصل بشيء آخر، حيث يقول الليث: "كل شيء اتصل بشيء فبينهما وصلة، أي اتصال وذريعة". كما يُقال:

---

[6] - محمد موفق الغلاييني، وسائل الاعلام وأثرها في وحدة الأمة ، دار المنارة ، 1985، ص 39.

[7] - عامر ابراهيم القندلجي الاعلام و المعلومات و الانترنت، عمان: دار اليازوري العلمية للنشر والتوزيع، 2013، ص 21.

"وصلت الشيء وصلاً ووَصْلة"، أي ربطته ولم أفصله. ويُستخدم مصطلح "الوصل" في مقابل "الهجران"، وهو نقيض "الفصل". وقد ورد في القرآن الكريم" :ولقد وصلنا لهم القول"، أي جمعنا بين أخبار الأنبياء وقصصهم بشكل متتابع لعلهم يتدبرون ويعتبرون.

واصطلاحا الاتصال هو عملية يقوم بها الفرد في سياق معين، يتم من خلالها نقل رسالة تحمل معلومات أو آراء أو مشاعر إلى الآخرين باستخدام رموز تعبيرية، بهدف تحقيق غايات محددة.

كما يُعرَّف بأنه عملية نقل وتبادل المعلومات، والأفكار، والمواقف، سواء بالكلام أو بالإشارات أو بالكتابة، وهو نشاط اجتماعي قائم على التعبير والتفاعل بين طرفين، يسعى إلى تحقيق أهداف محددة مسبقًا تنطوي على عنصر القصد والتدبير[8].

يُعرَّف الاتصال كذلك بأنه نقل المعلومات والمعاني والأفكار من شخص إلى آخر أو إلى مجموعة أفراد، بما يحقق الأهداف المنشودة داخل مؤسسة أو مجتمع ذي نشاط اجتماعي، مما يجعله بمثابة الروابط الديناميكية التي تصل بين أجزاء الهيكل التنظيمي لأي مؤسسة، سواء كان ذلك ضمن التنظيم الرسمي أو غير الرسمي.

أما من الناحية الإجرائية، فالاتصال يشمل جميع العمليات التي تتمثل في نقل المعلومات، والتجارب، والأنشطة العلمية والتربوية، سواء عبر الصوت أو الصورة أو الإشارات أو الكتابة، وعرضها بأسلوب متطور وفعال يهدف إلى تحقيق التفاعل بين المرسل والمتلقي، بما يسهم في إنجاح العملية التواصلية.

تُعرَّف تكنولوجيات الاتصال على أنها مجموعة من الأدوات والتقنيات والأنظمة الحديثة التي تُستخدم لتسهيل نقل وتبادل المعلومات بين الأفراد والمؤسسات عبر وسائل متعددة، مثل الشبكات الرقمية، والاتصالات السلكية واللاسلكية، والإنترنت، والأقمار الصناعية.

وارتبط مفهوم الاتصالات في وقت مضى بالاتصالات الهاتفية بسبب ربطه بالهاتف، ولكن هذا المفهوم توسع إلى ماوراء نطاق صناعة الهواتف، فالاتصالات اصبحت تعني مختلف عمليات ارسال واستقبال البيانات والمعلومات صور او اصوات او فيدوات عبر شبكات الاتصال وبصورة سلكية او لاسلكية.[9]

تُسهم هذه التكنولوجيات في تحسين جودة الاتصال، وتقليل المسافات الزمنية والجغرافية، مما يعزز التفاعل والتواصل الفعّال في مختلف المجالات، سواء على المستوى الشخصي أو المهني أو الحكومي. كما تلعب دورًا أساسيًا في تسريع تدفق المعلومات وتحقيق التكامل بين الوسائط التقليدية والرقمية، مما يدعم التحولات الاجتماعية والاقتصادية في العصر الرقمي.

ومن الضروري التمييز بين مفهومي الاتصال والتواصل؛ فالاتصال يشير إلى عملية نقل المعلومات أو الأفكار من مرسل إلى مستقبل عبر وسيلة معينة، وقد يكون أحادي الاتجاه أو

---

[8] - دحدوح منيه محاضرات ماده الاتصال في المؤسسه كليه العلوم الانسانيه والاجتماعيه جامعه 8 ماي 1945 قالمة السنة الجامعية 2015 2016 ، ص 09. ابراهيم عبد الله الزبيدي، العلاقات العامة والاعلام الرقابي، دار غيداء للنشر والتوزيع، 2017، ص 59.

[9] - حيدر شاكر البرزنجي، محمود حسن جمعة ، المرجع السابق، ص 22.

متبادلاً. أما التواصل، فيتسم بطبيعته التفاعلية، حيث يقوم الأطراف بتبادل الأفكار والمعلومات بشكل مستمر، مما يؤدي إلى تحقيق فهم مشترك. وبذلك، فإن استخدام مصطلح "الاتصال "هو الأكثر شيوعًا عند الإشارة إلى تكنولوجيات الإعلام والاتصال، لأنه يشمل عمليات نقل المعلومات عبر الوسائط الرقمية، سواء تمت في اتجاه واحد أو كانت تفاعلية بين الأطراف المختلفة.

خامسا: تعريف تكنولوجيا الاعلام والاتصال

بعد التعرف على مفاهيم التكنولوجيا، والإعلام، والاتصال بشكل منفصل، يمكننا القول إن تكنولوجيات الإعلام والاتصال هي دمج بين التكنولوجيا الحديثة ووسائل الإعلام وأساليب الاتصال، بهدف تسهيل نشر المعلومات وتعزيز التفاعل بين الأفراد والمؤسسات. فمع تطور التكنولوجيا، أصبحت وسائل الإعلام أكثر كفاءة، حيث تحول الإعلام التقليدي إلى إعلام رقمي، وأصبح الاتصال أكثر سرعة وتأثيرًا، مما أدى إلى ظهور ما يُعرف بـ "عصر المعلومات "أو "المجتمع الرقمي."

ومن كل ما سبق يمكن النظر إلى تكنولوجيات الإعلام والاتصال بمفهوم كامل على أنها نظام متكامل من الأدوات والتقنيات الحديثة المصممة لجمع البيانات ومعالجتها وتخزينها ونقلها باستخدام وسائل رقمية متطورة. وتشمل هذه التكنولوجيات الأجهزة الإلكترونية، والبرمجيات، والشبكات، والبنية التحتية الرقمية، التي تسهم في تسهيل عملية تبادل المعلومات وتعزيز فعالية الاتصال بين الأفراد والمؤسسات على المستوى العالمي.

سادسا: موقف المشرع الجزائري من تحديد مفهوم تكنولوجيات الاعلام والاتصال:

نظم المشرع الجزائري في القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[10] ولم يورد في محتواه تعريف صريح لمفهوم تكنولوجيات الإعلام والاتصال، ولكن يمكن استخلاصه من السياق العام للنصوص القانونية الواردة فيه. فالمشرع ركّز على تحديد المفاهيم الأساسية المرتبطة بالفضاء الرقمي، مثل المنظومة المعلوماتية، المعطيات المعلوماتية، والجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مما يعكس رؤيته لمجال تكنولوجيات الإعلام والاتصال باعتباره يشمل البنية التحتية الرقمية والأنظمة التقنية التي تتيح جمع المعلومات ومعالجتها وتخزينها ونقلها إلكترونيًا.

حيث عرّف المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بأنها:" جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات او أي جريمة اخرى ترتكب أو يُسهّل ارتكابها باستخدام منظومة معلوماتية أو نظام للاتصالات الإلكترونية". وتم تعريف "المنظومة المعلوماتية" في المادة الثانية بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو المترابطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذًا لبرنامج معين." أما المعطيات المعلوماتية فعرفها بانها :"أي عملية عرض للوقائع او المعلومات او المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شانها جعل منظومة معلوماتية تؤدي وظيفتها".

[10] - القانون الجزائري رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج العدد 47، تاريخ 16 اوت 2009، ص 05.

وبناءً على ذلك، يمكن فهم تكنولوجيات الإعلام والاتصال وفقًا للقانون الجزائري على أنها تشمل مجموعة الأنظمة المعلوماتية، وشبكات الاتصالات، والبرمجيات، والمعطيات الرقمية التي تُمكّن من إنشاء المعلومات الرقمية وتداولها عبر الوسائط التكنولوجية المختلفة، سواء كانت شبكات سلكية أو لاسلكية، أو أنظمة معالجة البيانات، أو منصات الاتصال الإلكتروني. كما أن المشرع الجزائري اعتبر هذه التكنولوجيات مجالًا ذا طبيعة حساسة، تستوجب حماية قانونية ضد الجرائم السيبرانية، من خلال وضع قواعد خاصة للوقاية والمكافحة، لا سيما فيما يتعلق بالمخاطر التي تهدد أمن المعلومات وسلامة المعاملات الرقمية.

ومن أمثلة هذه التكنولوجيات نذكر: الأنظمة الحاسوبية التي تعتمد على المعالجة الآلية للمعطيات، كأنظمة إدارة المؤسسات الرقمية. شبكات الاتصالات الإلكترونية **:مثل** شبكات الإنترنت، وشبكات الهاتف المحمول التطبيقات الرقمية **ك**واتساب، تليغرام ومنصات البريد الإلكتروني، أنظمة الترجمة الفورية، منصات الدفع الإلكتروني ، والتطبيقات المصرفية عبر الهاتف...وغيرها الكثير.

المطلب الثاني :خصائص ووظائف تكنولوجيات الإعلام والاتصال الحديثة.

أحدثت تكنولوجيات الإعلام والاتصال تحولًا جذريًا في طرق التواصل ونقل المعلومات، مما جعلها ضرورية في مختلف المجالات. لفهم دورها، يجب التمييز بين خصائصها التي تحدد طبيعتها، ووظائفها التي تعكس استخدامها في الحياة اليومية.

أولا: خصائص تكنولوجيات الإعلام والاتصال الحديثة.

تتمتع تكنولوجيا المعلومات والاتصالات بالعديد من الخصائص[11]، مما يجعلها محورًا أساسيًا في مختلف القطاعات مثل **الصحة، التعليم، التجارة، الأمن، والصناعة**، مما يساهم في تحسين جودة الحياة وتعزيز الكفاءة والإنتاجية.ومن هذه الخصائص مايلي:

1. **الأتمتة:** وتعني استخدام الأنظمة والبرامج الذكية لتنفيذ المهام التي كانت تُؤدى يدويًا، مما يقلل الجهد والوقت. مثال: أنظمة الروبوتات في المصانع التي تُجمّع السيارات تلقائيًا، أو أنظمة الذكاء الاصطناعي في الرد على استفسارات العملاء في البنوك.
2. **توفير الوقت:** تُمكّن تكنولوجيا المعلومات من إنجاز المهام بسرعة مقارنة بالطرق التقليدية، مما يزيد الكفاءة والإنتاجية. مثال: التحويلات المالية الإلكترونية التي تستغرق ثوانٍ مقارنة بإجراءات البنوك التقليدية التي قد تستغرق أيامًا.
3. **تقليص المكان:** يمكن للأفراد والمؤسسات العمل والتواصل من أي مكان دون الحاجة إلى مكاتب فعلية أو وسائل اتصال مادية. مثال: الاجتماعات الافتراضية عبر تطبيقات مثل **Zoom**و **Microsoft Teams**التي توفر بديلاً عن الاجتماعات الحضورية.
4. **اللاتزامنية:** تعني إمكانية التفاعل مع المعلومات في أي وقت دون الحاجة إلى أن يكون الطرفان متصلين في اللحظة نفسها. مثال: البريد الإلكتروني، حيث يمكن للشخص إرسال رسالة الآن، ويتلقى الرد لاحقًا في أي وقت يناسب المستقبل.

[11] - ابراهيم عمر يحياوي، المرجع السابق، ص 59 وما بعدها.

5. **التفاعلية:** تتيح التكنولوجيا للمستخدمين التفاعل الفوري مع المحتوى، مما يجعل الاتصال أكثر ديناميكية وحيوية. مثال: منصات التعلم الإلكتروني مثل **Moodle**، حيث يمكن للطلاب طرح الأسئلة والتفاعل مع المدرسين عبر المنتديات والاختبارات التفاعلية.

6. **الجماهيرية:** يمكن نشر المحتوى بسرعة والوصول إلى عدد كبير من الناس دون الحاجة إلى وسائل تقليدية مثل الصحف أو التلفاز. مثال: وسائل التواصل الاجتماعي مثل **Facebook**و **Twitter**التي تمكن الأفراد والمؤسسات من نشر الأخبار والمحتوى ليصل إلى ملايين المستخدمين.

7. **العالمية:** تمكن التكنولوجيا الأفراد والمؤسسات من التواصل والعمل عبر الحدود الجغرافية دون عوائق. مثال: شركات التجارة الإلكترونية مثل **Amazon**و **AliExpress**التي توفر البيع والشراء من أي مكان في العالم.

8. **الشيوع والانتشار:** أصبحت تكنولوجيا المعلومات والاتصالات متاحة بشكل واسع وسهل الاستخدام حتى لغير المختصين كما أن كثيرا منها يعد اقتصاديا غير مكلفا[12] . مثال: الهواتف الذكية التي تُمكّن الجميع من استخدام التطبيقات المختلفة بسهولة، مثل تطبيقات الدفع الإلكتروني والخدمات الحكومية عبر الإنترنت.

9. **القدرة على التخزين والاسترجاع:** تتيح أنظمة التخزين المتقدمة الاحتفاظ بكميات ضخمة من البيانات واسترجاعها عند الحاجة بسرعة. مثال: الخدمات السحابية مثل **Google Drive**و **Dropbox**التي توفر تخزين الملفات والوصول إليها من أي جهاز متصل بالإنترنت.

10. **التحديث المستمر:** التكنولوجيا في تطور مستمر، مما يحتم مواكبة التطورات لضمان أفضل أداء وأمان. مثال: تحديثات أنظمة التشغيل مثل **Windows**لتي تضيف ميزات جديدة وتحسن الأداء الأمني باستمرار.

11. **الأمن والخصوصية:** تتطلب التكنولوجيا إجراءات لحماية البيانات الشخصية من القرصنة والهجمات السيبرانية. مثال: استخدام بروتوكولات التشفير في المواقع الإلكترونية لحماية المعاملات البنكية والمراسلات.

12. **التكامل والتداخل:** تتيح التكنولوجيا ربط الأجهزة والأنظمة المختلفة معًا لتبادل البيانات والعمل بسلاسة. مثال: أنظمة المنازل الذكية التي تربط بين الإضاءة، التكييف، والكاميرات الأمنية، مما يمكن التحكم بها جميعًا عبر تطبيق واحد.

ثانيا: وظائف تكنولوجيات الإعلام والاتصال الحديثة.

تتميز الخصائص بكونها السمات الجوهرية التي تحدد طبيعة تكنولوجيا المعلومات والاتصالات، مثل الأتمتة، التفاعلية، واللاتزامنية. أما **الوظائف** فهي التطبيقات العملية لهذه الخصائص، أي الأدوار التي تؤديها التكنولوجيا في مختلف المجالات، مثل التعليم، التجارة، والإعلام. بمعنى آخر، الخصائص هي **كيف تعمل التكنولوجيا؟**، بينما الوظائف هي **ما الذي يمكن أن تفعله التكنولوجيا؟ ومن** أهم وظائف تكنولوجيا المعلومات والاتصال:

[12] - منصر خالد، 2012، ص 67

1. **نقل المعلومات** :تُمكّن تقنيات الاتصال الحديثة من إرسال البيانات والمعلومات بسرعة عبر مختلف الوسائل[13]، مثل البريد الإلكتروني، تطبيقات المراسلة الفورية، والإنترنت.
2. **التعليم والتدريب عن بعد** :توفر منصات التعلم الإلكتروني بيئة تفاعلية تمكّن الطلاب من الدراسة عن بُعد عبر الدروس المسجلة أو الحصص المباشرة، مثل منصات Coursera وMoodle.
3. **التجارة الإلكترونية** :تسهم التكنولوجيا في تسهيل عمليات البيع والشراء عبر الإنترنت، مما يعزز التجارة الرقمية من خلال المتاجر الإلكترونية مثل Amazon و eBay.
4. **الإعلام الرقمي** :تمكن تكنولوجيا المعلومات من نشر الأخبار والمحتوى الإعلامي بسرعة عبر مواقع الأخبار ووسائل التواصل الاجتماعي مثل YouTube و Facebook.
5. **الخدمات الحكومية الإلكترونية** :تتيح للمؤسسات الحكومية تقديم خدماتها للمواطنين عبر الإنترنت، مثل استخراج الوثائق الرسمية، دفع الضرائب، وحجز المواعيد.
6. **الأمن السيبراني** :تستخدم التكنولوجيا لحماية البيانات والمعلومات من القرصنة والهجمات الإلكترونية، من خلال أنظمة التشفير والجدران النارية.
7. **إدارة البيانات وتحليلها** :تساعد تقنيات تخزين البيانات وتحليلها في تحسين صنع القرار من خلال قواعد البيانات الضخمة وأنظمة الذكاء الاصطناعي.
8. **الصحة الرقمية** :توفر حلولًا تقنية في المجال الصحي، مثل الاستشارات الطبية عن بعد، السجلات الصحية الإلكترونية، والتطبيقات الذكية لمتابعة اللياقة والصحة.
9. **الصناعة والإنتاج** :تعتمد المصانع على الأنظمة الرقمية والأتمتة في تحسين الإنتاجية والجودة، من خلال الروبوتات الصناعية والتحكم الذكي في خطوط الإنتاج.
10. **الترفيه الرقمي** :توفر تكنولوجيا المعلومات مجموعة واسعة من وسائل الترفيه مثل الألعاب الإلكترونية، خدمات البث المباشر للأفلام والموسيقى، والتواصل عبر الواقع الافتراضي.

المطلب الثالث: التطور التاريخي لتكنولوجيات الإعلام والاتصال.

تعد تكنولوجيا الإعلام والاتصال من أبرز مظاهر التقدم البشري في العصر الحديث، وقد شهدت هذه التكنولوجيا تطورات متسارعة منذ بداية العصر الصناعي وحتى العصر الرقمي الحالي. يعكس هذا التطور تحولًا جذريًا في طرق نقل المعلومات والتفاعل الاجتماعي والثقافي بين الأفراد والمجتمعات. نستعرض في هذا الموضوع التطور التاريخي لتكنولوجيات الإعلام والاتصال بموجب مراحل رئيسية وعناوين بارزة.

1.المرحلة الأولى: وسائل الإعلام التقليدية (قبل القرن 19)

قبل اختراع الآلات الحديثة، كان الاتصال يعتمد على الوسائل التقليدية مثل الرسائل المكتوبة، والنقل الشفهي، ووسائل البث البدائية مثل الطبول والإشارات. كانت هذه الوسائل محدودة في نطاق استخدامها، ومرتبطًا بمناطق جغرافية محدودة، كما كانت تحتاج إلى زمن طويل لنقل المعلومات من مكان إلى آخر.

- **الكتابة والمراسلات اليدوية** :كانت المحادثات والخطب العامة وسيلة أساسية للتواصل بين الناس في المجتمع القديم.

[13] - ابراهيم عمر يحياوي، المرجع السابق، ص 68.

• **النقل عبر البريد :**بدأ استخدام البريد كأداة لنقل الرسائل الرسمية والشخصية، مما ساعد على تحسين مستوى الاتصال بين المدن والدول.

.2المرحلة الثانية: اختراعات القرن 19 (منذ الثورة الصناعية)

شهد القرن 19 تطورًا كبيرًا في وسائل الاتصال، نتيجة للثورة الصناعية التي جلبت معها اختراعات غيرت جذريًا الطريقة التي ينتقل بها البشر والمعلومات. أبرز الاختراعات في هذه المرحلة كانت:

• **اختراع التلغراف (1837)[14]:** يُعتبر اختراع التلغراف على يد صامويل مورس من أهم معالم هذه الحقبة. سمح التلغراف بنقل الرسائل بسرعة عبر أسلاك كهربائية، وهو ما أحدث نقلة نوعية في التواصل بين الدول والمناطق البعيدة.

• **اختراع الهاتف (1876) :**قدم ألكسندر غراهام بيل اختراع الهاتف[15]، الذي سمح بنقل الصوت البشري على مسافات طويلة باستخدام الأسلاك الكهربائية. شكل الهاتف بداية لمرحلة جديدة من التواصل المباشر بين الأفراد.

• **الصحافة والطباعة :** الطباعة تم اختراعها بالفعل في منتصف القرن الخامس عشر، وبالتحديد في عام 1450 تقريبًا بواسطة يوهان غوتنبرغ في ألمانيا. اختراع غوتنبرغ للطباعة الميكانيكية كان ثورة حقيقية في تاريخ الإعلام، حيث أصبحت الكتب والمطبوعات أكثر قدرة على الانتشار. وهذا الاختراع مهد الطريق لإنتاج الكتب والمطبوعات على نطاق واسع، وبالتالي أدى إلى تطور الصحافة بشكل ملموس. ويُعتبر العديد من المؤرخين أن أول صحيفة حديثة هي "The Relation"، التي نُشرت في ألمانيا عام 1605. كان ذلك خلال فترة ما بعد اختراع الطباعة، وكان هذا الاختراع يمثل نقلة كبيرة في نشر الأخبار والمعلومات. وفي القرن التاسع عشر، مع الثورة الصناعية وانتشار الطباعة بشكل أسرع وأكثر دقة، ظهرت الصحف اليومية والمجلات في معظم البلدان الغربية.

.3المرحلة الثالثة: ظهور الإعلام السمعي البصري (القرن 20)

في القرن العشرين، شهد العالم تحولًا كبيرًا في تكنولوجيا الإعلام والاتصال، مما أدى إلى تطور وسائل الإعلام السمعي البصري. خلال هذه الفترة، ظهرت مجموعة من الابتكارات التي ساعدت على تغيير مفهوم الاتصال بشكل جذري.

• **الإذاعة (1920)** ظهرت أولى محطات الإذاعة في عشرينيات القرن الماضي، وأصبحت الإذاعة من أهم وسائل الإعلام التي تتيح الوصول إلى جمهور واسع بسرعة. وفرت الإذاعة وسيلة فعالة لنقل الأخبار والمعلومات والترفيه للمجتمعات[16].

• **التلفزيون (1930-1950):** كان اختراع التلفزيون نقطة تحول كبيرة في عالم الإعلام. سمح التلفزيون ببث الصور والصوت في وقت واحد، مما جعل الإعلام أكثر تأثيرًا على الجمهور. مع مرور الوقت، أصبح التلفزيون الوسيلة المهيمنة في نقل الأخبار والترفيه.

---

[14] - فتحي حسين عامر، وسائل الاتصال الحديثة من الجريدة الى الفيسبوك، 2011، ص 43.

[15] - عامر ابراهيم القندلجي الاعلام و المعلومات و الانترنت،

[16] - نظام الاتصال والاعلام الدولي، تكنولوجيا الاتصال والمعلومات وتاثيرها على سيادة الدولة ، ص 88.

• **الأقمار الصناعية (1960-1970) :**تطور تكنولوجيا الأقمار الصناعية سمح ببث إشارات التلفزيون والإذاعة عبر مسافات بعيدة، مما جعل الإعلام العالمي أكثر تواصلًا. أسهم ذلك في ظهور شبكة الإعلام العالمية والقدرة على بث الأخبار والبرامج بشكل عالمي. كما اصبحت الاقمار الصناعية تستخدم كذلك في تقل المعلومات والبيانات مما يساهم في ربط العالم بعضه ببعض وتوفير حلول تقنية متطورة للمناطق التي يصعب الوصول إليها عبر وسائل الاتصال التقليدية[17].

.4المرحلة الرابعة: العصر الرقمي (منذ أواخر القرن 20 وحتى الآن)

منذ ظهور الحاسوب الشخصي وتكنولوجيا الإنترنت، شهدت تكنولوجيا الإعلام والاتصال تحولًا كبيرًا، حيث أصبح بالإمكان نشر واستقبال المعلومات بشكل فوري وعلى نطاق واسع. وهذا العصر الذي بدأ في أواخر القرن 20 استمر في التطور ليحدث تغييرات عميقة في كافة جوانب الحياة البشرية.

• **الإنترنت (1990) :** ان ظهور الإنترنت في التسعينيات بمثابة ثورة في الإعلام. أتاح الإنترنت للأفراد والمؤسسات الوصول إلى كميات ضخمة من المعلومات في أي وقت ومن أي مكان[18]. كما أنشأ الإنترنت العديد من منصات التواصل الاجتماعي مثل فيسبوك وتويتر ويوتيوب، التي أصبحت جزءًا لا يتجزأ من حياة الناس اليومية.

• **الهواتف الذكية (2000) :** في بداية الألفية الجديدة، أصبح الهاتف الذكي هو الأداة الرئيسية للوصول إلى الإنترنت، وتوافر التطبيقات التي تسمح بالتواصل عبر الإنترنت، بما في ذلك الرسائل النصية، والمكالمات الصوتية والفيديو، والوسائط الاجتماعية. هذا التطور جعل الاتصال أكثر مرونة وسهولة.

• **الإعلام الاجتماعي والتفاعل الرقمي :**من خلال منصات مثل فيسبوك، تويتر، وإنستغرام، أصبح الأفراد قادرين على إنشاء محتوى إعلامي والتفاعل مع الآخرين بشكل غير مسبوق. أصبحت هذه المنصات الوسيلة الرئيسية للتفاعل بين الناس[19].

.5المرحلة الخامسة: تطور الذكاء الاصطناعي ووسائل الإعلام المستقبلية

في السنوات الأخيرة، بدأت التقنيات الحديثة مثل الذكاء الاصطناعي (AI) والواقع الافتراضي (VR) في تغيير وجه الإعلام والاتصال بشكل جذري. بدأت هذه التقنيات في التفاعل مع المستخدمين بشكل يتسم بالذكاء والمرونة.

• **الذكاء الاصطناعي في الإعلام :**أصبح الذكاء الاصطناعي يستخدم لتحليل البيانات الكبيرة، وإنشاء محتوى مخصص للمتلقي. تعمل الخوارزميات على تحسين التجربة الرقمية، مثل توجيه الإعلانات والمواضيع الأكثر ملاءمة للمستخدم.

• **الواقع المعزز والافتراضي :**بدأت هذه التقنيات في تغيير طريقة استهلاك المحتوى الإعلامي. يسمح الواقع المعزز بإضافة عناصر رقمية إلى العالم الحقيقي، بينما يتيح الواقع الافتراضي تجربة وسائل الإعلام في بيئات ثلاثية الأبعاد بالكامل

---

[17] - ياسر عبد الرحمن خلف ، تكنولوجيا الاعلام والاتصالات، الجنادرية للتوزيع والنشر، الطبعة الأولى ، 2017، ص28.

[18] - خليل صابات ، جما عبد العظيم، وسائل الاتصال نشاتها وتطورها، مكتبة الانجلو مصرية، ص 522.

[19] - عمر عبد العزيز هلال، وسائل التواصل الاجتماعي واحكامها في الفقه الاسلامي، دار الكتب العلمية، ص 59..

المبحث الثاني: الثورة الرقمية وانعكاساتها القانونية

أدى التقدم التكنولوجي السريع الذي شهدته العقود الأخيرة إلى نشوء ثورة رقمية شاملة، مست مختلف أوجه الحياة المعاصرة، من الإدارة إلى الاقتصاد، ومن العلاقات الاجتماعية إلى ممارسة الحقوق والحريات. ومع هذا التحول العميق، ظهرت تحديات قانونية جديدة تفرض على المشرعين والقانونيين التفكير في إعادة صياغة العديد من المفاهيم القانونية الكلاسيكية لمواكبة الواقع الرقمي المتسارع. فالفضاء السيبراني بات يشكل بيئة جديدة تنشأ فيها علاقات قانونية معقدة تتطلب أطرًا تشريعية وتنظيمية تتسم بالمرونة والتجدد. ومن هذا المنطلق، يسعى هذا المبحث إلى تحليل الأبعاد القانونية لهذه الثورة الرقمية، من خلال التطرق إلى الآثار المباشرة على الحقوق الأساسية، والإشكالات المرتبطة باستخدام التكنولوجيا، وكذا الجهود التنظيمية الوطنية والدولية الرامية إلى ضبط هذا المجال وضمان توازنه مع المبادئ القانونية والحقوقية.

المطلب الأول: الأبعاد القانونية للتحول الرقمي وحماية الحقوق في البيئة الرقمية

يشكل التحول الرقمي أحد أبرز ملامح العصر الحديث، حيث أصبحت التكنولوجيا الرقمية متغلغلة في مختلف القطاعات، ما أثر بشكل مباشر على طبيعة الحقوق والحريات، وأنماط المعاملات، ومجالات المسؤولية. وقد أفرز هذا الواقع مستجدات قانونية تتعلق أساسًا بكيفية حماية حقوق الإنسان في البيئة الرقمية، والحفاظ على سرية البيانات، ومكافحة الجرائم السيبرانية، إلى جانب تنظيم العقود والتجارة الإلكترونية، ومواكبة التطورات المتسارعة في مجال الذكاء الاصطناعي. وانطلاقًا من هذه الاعتبارات، يتناول هذا المطلب عدة محاور فرعية تهدف إلى رصد الأبعاد القانونية الأكثر ارتباطًا بالتحول الرقمي، من خلال تحليل تأثيراته على الحقوق الأساسية، ودراسة التحديات المرتبطة بالخصوصية وأمن المعلومات، إلى جانب مناقشة الإطار القانوني المنظم للمعاملات الرقمية، والذكاء الاصطناعي.

أولا: تأثير التطور التكنولوجي على حقوق الإنسان

شهدت حقوق الإنسان تحولات كبيرة نتيجة لتطور تكنولوجيات الإعلام والاتصال، حيث أصبحت التكنولوجيا تشكل جزءاً أساسياً من حياة الأفراد، ومن أبرز الآثار القانونية التي ظهرت:

.1حق الخصوصية وحمايته: لقد أصبح حق الخصوصية مهددًا بسبب التكنولوجيا الحديثة[20]. فعلى سبيل المثال، أصبح من السهل جمع البيانات الشخصية للأفراد من خلال الإنترنت، وكذلك مراقبة الأنشطة الرقمية من خلال الأجهزة المحمولة والموقع الجغرافي. الأمر الذي يتطلب من التشريعات حماية الحق في الخصوصية من خلال آليات قانونية صارمة مثل حماية البيانات الشخصية.

[20] - فاضلي سيد عي، آثار التطور التكنولوجي على حماية الحق في الخصوصية في النظام الاروربي لحماية حقوق الانسان، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، ةالسنة 2020، ص 1638.

.2حرية التعبير: من جهة أخرى، يمكن أن تساهم التكنولوجيا في تعزيز حرية التعبير عبر الإنترنت من خلال منصات التواصل الاجتماعي، إذ أصبح الأفراد قادرين على التعبير عن آرائهم ونشرها بحرية. ولكن، في المقابل، تثير هذه الحرية العديد من القضايا القانونية، مثل قضايا التشهير، خطاب الكراهية، ونشر المعلومات المغلوطة.

.3الحق في الوصول إلى المعلومات: يعد التطور التكنولوجي خطوة كبيرة في تحقيق الحق في الوصول إلى المعلومات. حيث أصبح الأفراد قادرين على الحصول على معلومات من جميع أنحاء العالم في لحظات، مما يعزز من الشفافية والمشاركة العامة في الحياة السياسية والاجتماعية.

ثانيا: تكنولوجيات الإعلام والاتصال وسرية البيانات

مع التقدم السريع في تكنولوجيا الإعلام والاتصال، ازدادت التحديات المرتبطة بسرية البيانات وحمايتها، لا سيما مع توسع استخدام المنصات الرقمية في التجارة الإلكترونية، والتواصل الاجتماعي، وتطبيقات الذكاء الاصطناعي. فقد أدى هذا التطور إلى تصاعد المخاوف بشأن كيفية جمع البيانات وتخزينها واستغلالها، خاصة في ظل التهديدات المتزايدة لخصوصية الأفراد والمؤسسات.

تشمل هذه التهديدات عمليات اختراق البيانات الشخصية وبيعها في الأسواق السوداء، مما يعرض المستخدمين لانتهاكات خطيرة تمس خصوصياتهم، فضلاً عن تزايد عمليات القرصنة الإلكترونية التي تستهدف المؤسسات الكبرى. وللتصدي لهذه المخاطر، برزت الحاجة إلى وضع قوانين صارمة لحماية البيانات، تفرض ضوابط واضحة على طرق جمعها واستخدامها، وتحد من الاستغلال غير المشروع لها، خصوصًا مع الانتشار الواسع لتقنيات الذكاء الاصطناعي التي تعتمد على البيانات الضخمة.

في هذا السياق، تلعب تقنيات التشفير دورًا جوهريًا في تأمين نقل البيانات عبر الشبكات الرقمية، حيث توفر الحماية ضد الاختراقات والتجسس[21]. كما أن المؤسسات مطالبة باستخدام أدوات تأمين متقدمة للحفاظ على سرية المعلومات وحماية حقوق المستخدمين. وعلى الرغم من الجهود التشريعية المبذولة، لا تزال هناك تحديات كبيرة في مواجهة الانتهاكات الرقمية، مثل سرقة الهوية والاستغلال غير القانوني للبيانات، مما يستلزم مزيدًا من التطوير القانوني والتكنولوجي لضمان بيئة رقمية آمنة.

ثالثا: الجرائم الإلكترونية والقوانين الجنائية

تُعد الجرائم الإلكترونية من أخطر التحديات القانونية التي أفرزتها الثورة الرقمية[22]، إذ أدى الانتشار الواسع للإنترنت إلى تسهيل العديد من الأنشطة غير القانونية، مثل القرصنة الإلكترونية التي تستهدف اختراق الأنظمة والبيانات، والاحتيال الإلكتروني الذي يشمل عمليات النصب

[21] - الاتجاهات العالمية في حرية التعبير وتنمية وسائل الاعلام: تركيز خاص على الوسائل الرقمية في عام 2015، منشورات اليونسكو ، منظمة الامم المتحدة للتربية والعلم والثقافة، ص 21.

[22] - مقدم شبيلة . مقناني صبرينة تأثير الجرائم الالكترونية على المعلومات الرقمية المجلة الجزائرية للأبحاث والدراسات، المجلد 03، العدد 01، 2020، ص 137 وما بعدها..

والابتزاز السيبراني، بالإضافة إلى نشر المحتويات غير القانونية كالمواد الإباحية أو المعلومات المضللة التي تهدد استقرار المجتمعات.

ولمواجهة هذه التهديدات، تم تطوير منظومات قانونية متخصصة تهدف إلى الحد من الجرائم الإلكترونية، حيث تُفرض عقوبات صارمة على اختراق البيانات وتعطيل الأنظمة، كما سُنَّت قوانين لمكافحة الأخبار الزائفة للحد من تأثير المعلومات المغلوطة على الرأي العام، نظراً لما يمكن أن تسببه من اضطرابات اجتماعية وسياسية. ومع تزايد تعقيد الجرائم السيبرانية، تبرز الحاجة المستمرة إلى تحديث القوانين وتطوير تقنيات الحماية لتعزيز الأمن الرقمي وضمان بيئة إلكترونية أكثر أماناً.

رابعا: التجارة الإلكترونية والعقود الرقمية

أدى التطور الرقمي إلى ازدهار التجارة الإلكترونية، مما استلزم وضع إطار قانوني ينظم المعاملات التجارية عبر الإنترنت ويضمن حقوق جميع الأطراف. فقد أصبح من الضروري سن قوانين تنظم هذا القطاع، مثل تشريعات التجارة الإلكترونية التي تحدد القواعد القانونية للشراء والبيع عبر المنصات الرقمية، وتفرض معايير لحماية المستهلك وضمان الشفافية في التعاملات[23].

كما برزت العقود الرقمية كأداة قانونية أساسية في هذا المجال، حيث يعتمد إبرام الاتفاقيات التجارية على التوقيع الإلكتروني والتوثيق الرقمي لضمان مصداقية وسلامة المعاملات. ومع التطور المستمر للتكنولوجيا، بات من المهم تحديث هذه القوانين باستمرار لمواكبة التغيرات وضمان بيئة تجارية رقمية آمنة وعادلة.

خامسا: التحديات القانونية المرتبطة بتطور الذكاء الاصطناعي

مع التطور المتسارع لتكنولوجيات الإعلام والاتصال، أصبح الذكاء الاصطناعي عنصرًا أساسيًا في هذه التحولات الرقمية، وأدى استخدامه إلى تهديد الخصوصية والامن الالكتروني، حيث يمكن ان يتم من خلاله جمع وتحليل البيانات الشخصية للمستخدمين دون علمهم و موافقتهم، مما يشكل تهديدا لخصوصيتهم وامنهم الالكتروني[24]، مما أدى إلى بروز تحديات قانونية معقدة تتطلب تنظيمًا دقيقًا لضمان الاستخدام المسؤول لهذه التكنولوجيا. ومن أبرز الإشكاليات القانونية التي أثارها الذكاء الاصطناعي مسألة حقوق الملكية الفكرية، حيث أصبح من الضروري تحديد الجهة التي تمتلك الحقوق المرتبطة بالأنظمة الذكية، لا سيما في ظل مساهمة الذكاء الاصطناعي في تطوير المحتوى الرقمي والإبداعي. فمع قدرته على إنتاج نصوص، صور، وبرمجيات متطورة، تثار تساؤلات قانونية جوهرية حول ما إذا كان الابتكار يعود للمطور البشري، أم للنظام الذكي ذاته، أم للجهة المالكة للتكنولوجيا المستخدمة.

إضافةً إلى ذلك، فإن اندماج الذكاء الاصطناعي في مجالات حساسة مثل الصحافة الرقمية، الأمن السيبراني، والخدمات الذكية يفرض تساؤلات قانونية حول المسؤولية القانونية عند وقوع

---

[23] - عبد الصبورعبد القوي علي مصري، التنظيم القانوني للتجارة الالكترونية ، مكتبة القانون والاقتصاد، الرياض، ص137.

[24] - هالة احمد الحسيني، دعاء هشام جمعة ، الذكاء الاصطناعي وتوظيفه في المؤسسات الإعلامية، العربي للنشر والتوزيع، ص 35.

أخطاء أو أضرار ناجمة عن قرارات هذه الأنظمة. فمثلًا، في حال نشر أخبار زائفة عبر منصات مدعومة بالذكاء الاصطناعي، أو اتخاذ قرارات خاطئة في الأنظمة التنبؤية، يظل من الصعب تحديد المسؤولية القانونية بين المبرمج، المستخدم، أو الشركة المطورة. لذا، بات من الضروري تطوير أطر قانونية واضحة لتحديد المسؤوليات وضمان عدم انتهاك الحقوق الفردية أو الجماعية.

علاوةً على ذلك، يفرض تطور الذكاء الاصطناعي تحديات متزايدة فيما يتعلق بتنظيمه ورقابته في ظل تكنولوجيات الإعلام والاتصال الحديثة. إذ إن الاستخدام المتزايد للخوارزميات في تحليل البيانات الضخمة والتفاعل مع المستخدمين قد يؤدي إلى انتهاكات خطيرة للخصوصية كما اشرنا سابقا، ومن هنا، تبرز الحاجة إلى وضع تشريعات تواكب هذه التطورات التكنولوجية، بحيث تحقق التوازن بين الاستفادة من إمكانات الذكاء الاصطناعي وتعزيز الحماية القانونية للأفراد والمؤسسات في الفضاء الرقمي.

المطلب الثاني: الاطار القانوني لتنظيم التكنولوجيا الرقمية

نظرًا للتحديات التي فرضتها الثورة الرقمية، طورت العديد من الدول والمنظمات الدولية تشريعات لتنظيم الفضاء السيبراني، وقطاع تكنولوجيا الالعلام والاتصال، والجزائر لم تكن بمنأى من ذلك:

أولا: التشريعات الدولية والوطنية لتنظيم الجوانب القانونية لتكنولوجيات الاعلام والاتصال.

تمكنت التشريعات الدولية من متابعة التطورات السريعة في تكنولوجيا الإعلام والاتصال عبر عدة مراحل هامة. منذ بداية القرن العشرين، بدأ الاهتمام بتوحيد المعايير القانونية لحماية حقوق المؤلف. في **9**سبتمبر 1886، تم توقيع اتفاقية برن لحماية المصنفات الأدبية والفنية[25]، التي وضعت الأساس لحماية حقوق المؤلف على المستوى الدولي. كانت هذه الاتفاقية خطوة مهمة في تأطير حقوق المبدعين في ظل تطور وسائل الاتصال والنشر، وافتتحت الطريق لحماية المصنفات الرقمية في العصر الحديث.

وفي 15مايو 1932، تم توقيع اتفاقية جنيف للاتصالات التي نظمت الاتصالات بين الدول، مشيرة إلى أهمية تيسير الاتصالات بين الدول باستخدام الوسائل الحديثة المتاحة آنذاك. ورغم أنها لم تكن تشريعات رقمية مباشرة، فإن الاتفاقية شكلت إطارًا تنظيميًا للأمور التي ستصبح فيما بعد أساسية في تنظيم الإنترنت والاتصالات الرقمية.

تدريجيًا، ومع ظهور الإنترنت والتطورات الجديدة في تكنولوجيا الإعلام والاتصال، بدأت قضايا حماية حقوق الإنسان تأخذ مكانة بارزة. في 10ديسمبر 1948، أصدرت الأمم المتحدة إعلان حقوق الإنسان[26]، الذي نص على حماية حق الأفراد في الخصوصية، وهو ما أصبح فيما بعد أحد الأسس الرئيسية للحفاظ على حقوق الأفراد في الفضاء الرقمي. هذا الإعلان أتاح إطارًا قانونيًا يتم تطويره لاحقًا لمواجهة انتهاكات الخصوصية في الفضاء الإلكتروني.

---

[25] - الغمري محمد، الملكية الفكرية ، ببلومانيا للنشر والتوزيع، ص27.

[26] - سمير شوقي، دور الإعلان العالمي لحقوق الإنسان في تدويل حماية الشخصية الانسانية، مجلة تحولات المجلد 02 العدد 01، ص 87وما بعدها.

في مجال مكافحة الجرائم الرقمية، شكل اتفاقية بودابست بشأن الجرائم الإلكترونية، التي اعتمدت في 23نوفمبر 2001، نقطة تحول مهمة في كيفية تصدي القوانين الدولية للأنشطة غير القانونية على الإنترنت. كانت هذه الاتفاقية أول اتفاقية دولية تركز بشكل خاص على التصدي للجرائم الإلكترونية مثل القرصنة الإلكترونية والتلاعب بالبيانات. وتضمنت بنودًا تتيح التعاون بين الدول لمكافحة الجرائم عبر الإنترنت[27].

ثم ظهرت الحاجة إلى تنظيم قضايا حماية البيانات الشخصية في ظل الاستخدام المتزايد للإنترنت. في **24**أكتوبر 199**5**، أقر الاتحاد الأوروبي التوجيه EC 46/95/بشأن حماية البيانات الشخصية، والذي وضع الأسس القانونية لحماية المعلومات الشخصية للمواطنين داخل دول الاتحاد الأوروبي. هذه الخطوة مثلت تحركًا حاسمًا نحو وضع أطر قانونية شاملة لحماية الخصوصية في عصر الإنترنت[28].

بالإضافة إلى ذلك، وفي إطار حماية خصوصية الأطفال في البيئة الرقمية، أصدر الكونغرس الأمريكي في **21**أكتوبر 1998 قانون حماية خصوصية الأطفال على الإنترنت .**(**COPPA) هذا القانون كان أول تشريع من نوعه في الولايات المتحدة، حيث فرض على المواقع الإلكترونية الحصول على موافقة الوالدين قبل جمع أي معلومات شخصية من الأطفال دون سن 13 عامًا.

ومع تطور تقنيات الإنترنت، ظهرت الحاجة إلى قوانين تعالج الأنشطة غير القانونية على الشبكات العميقة. في **2012**، تم إصدار قانون الشبكة العميقة في الولايات المتحدة، الذي استهدف التعامل مع الأنشطة غير المشروعة على الشبكات المظلمة، مثل تداول المواد الممنوعة أو المخدرات.

في **2018**، صدر قانون حماية البيانات الشخصية في الهند، الذي يحاكي في بعض جوانبه اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، ويهدف إلى تنظيم جمع واستخدام البيانات الشخصية داخل الهند. أصبح هذا التشريع أحد أبرز القوانين التي تعكس الجهود العالمية لحماية الخصوصية في العصر الرقمي[29].

كما أصدرت المملكة المتحدة في **27مارس 2018**قانون حماية الخصوصية الرقمية .(Digital Privacy Act)هذا القانون يهدف إلى حماية المستخدمين من تهديدات الخصوصية الرقمية في عصر الإنترنت، حيث يتطلب من الشركات التقنية والمؤسسات الرقمية التأكد من أن البيانات الشخصية للمواطنين محفوظة بشكل آمن، مع تعزيز الشفافية في كيفية جمع البيانات واستخدامها. كما يولي أهمية خاصة لحماية الأطفال على الإنترنت.

وفي **25مايو 2018**، تم تطبيق اللائحة العامة لحماية البيانات **(GDPR)** من قبل الاتحاد الأوروبي، التي تعد واحدة من أبرز التشريعات الحديثة في هذا المجال. فرضت اللائحة شروطًا

---

[27] - منال البلقاسي، تأمين التعهديات السبرانية تحت المجهر الرقمي، العبيكان للنشر، الرياض،2024، ص 208.

[28] - المرجع نفسه ، ص 209.

[29] - منال البلقاسي، المرج السابق، ص 229.

صارمة على الشركات التي تتعامل مع البيانات الشخصية، حيث تطلب موافقة الأفراد قبل جمع بياناتهم، كما منح الأفراد حق الوصول إلى بياناتهم وتصحيحها أو حذفها[30].

في **2019**، أقرَّت فرنسا قانون الأمن السيبراني الذي يهدف إلى تعزيز الأمان الرقمي للبلاد وتوفير حماية للبنية التحتية الحيوية من الهجمات الإلكترونية. يتطلب القانون من الشركات الفرنسية التي تتعامل مع أنظمة حيوية مثل الطاقة والنقل والاتصالات اتخاذ تدابير أمنية صارمة لحماية هذه الأنظمة من الهجمات السيبرانية. كما يتم فرض عقوبات على الشركات التي تتخلف عن الالتزام بهذه التدابير.

أخيرًا، وفي **15فبراير 2023**، تم إصدار قانون الذكاء الاصطناعي في الاتحاد الأوروبي **(AI Act)**، الذي يُعد أول تشريع شامل في الاتحاد الأوروبي لتنظيم الذكاء الاصطناعي. يهدف هذا القانون إلى ضمان استخدام هذه التكنولوجيا بشكل آمن وأخلاقي، حيث يشمل متطلبات للشفافية والمساءلة وضمان سلامة الأفراد من مخاطر استخدام الذكاء الاصطناعي في مختلف المجالات.

ثانيا: التنظيم القانوني لتكنولوجيات الإعلام والاتصال في الجزائر

يعد أمر رقم 75-89 المؤرخ في 30 ديسمبر سنة 1975[31] بمثابة أول تنظيم قانوني للبريد والمواصلات في الجزائر، وهو يمثل الأسس الأولى التي تحكم خدمات البريد والمواصلات في البلاد في فترة ما قبل الثورة التكنولوجية الحديثة. لم يكن هذا الأمر يشمل سوى البريد التقليدي والمواصلات عبر الأسلاك والاتصالات السلكية البسيطة، التي كانت تقتصر على التبادل البريدي الداخلي والخارجي على مستوى محدود. وفي هذا السياق، كان القطاع يعتمد على أساليب التواصل التقليدية، مثل الرسائل الورقية، وكانت الخدمات محدودة في نطاقها الجغرافي والزمني. لكن هذا القانون وضع القواعد الأولية التي تؤطر النظام البريدي والمواصلاتي في الجزائر ويشكل بداية التشريع الجزائري في هذا المجال.

ومع بداية القرن الجديد، وتزايد الاعتماد على الإنترنت كأداة أساسية في الحياة اليومية، جاء أمر رقم 2000-03 المؤرخ في 05 غشت سنة 2000 [32] ليحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية في الجزائر. على الرغم من أن هذا الأمر كان استمرارًا للأمر السابق، إلا أنه كان يتسم بتحديثات مهمة تتماشى مع ظهور الإنترنت وتقنيات الاتصال الحديثة. وكان هذا القانون بمثابة خطوة نحو تنظيم قطاع الاتصالات بشكل شامل، بما يشمل الإنترنت، والهواتف المحمولة، والخدمات السلكية واللاسلكية. بالإضافة إلى ذلك، بدأ هذا القانون في معالجة الجوانب المتعلقة بتطوير البنية التحتية للاتصالات وفتح المجال أمام شركات القطاع الخاص لتقديم خدمات جديدة وذات جودة عالية للمستهلكين. كما ساهم في تعزيز الرقابة على سوق الاتصالات وضمان حقوق المستهلك.

---

[30] - عادل عبد الصادق، البيانات الشخصية الصراع على نفط القرن الحادي والعشرين، المركز العربي لأبحاث الفضاء الالكتروني، 2018، ص 39.

[31] - أمر رقم 75-89 المؤرخ في 30 ديسمبر سنة 1975 و المتضمن قانون البريد و المواصلات

[32] - أمر رقم 2000-03 المؤرخ في 05 غشت سنة 2000 يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية. ج ر رقم 48 المؤرخة في 06 اوت 2000

ثم صدر عن المشرع الجزائري القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009[33] من القوانين المهمة في تنظيم الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال. في ضوء الثورة الرقمية التي كانت تشهدها الجزائر، وخاصة مع التوسع الكبير في استخدام الإنترنت والتقنيات الحديثة، أصبح من الضروري وضع إطار قانوني شامل لمكافحة الجرائم الإلكترونية. هذا القانون تناول بالتحليل الأبعاد القانونية للجرائم التي تحدث في الفضاء الرقمي، مثل القرصنة الإلكترونية، الاحتيال الإلكتروني، والتشهير عبر الإنترنت. كما قام بتعريف الجرائم المرتبطة باستخدام تكنولوجيا المعلومات، وحدد العقوبات المناسبة لكل نوع من الجرائم. شكل هذا القانون خطوة هامة نحو مواجهة التحديات التي نشأت مع تطور تكنولوجيا الإعلام والاتصال، وبالتالي حماية الأفراد والمجتمع من الأضرار الناجمة عن سوء استخدام التكنولوجيا.

ولغرض تحديد القواعد العامة للتوقيع والتصديق الإلكترونيين صدر القانون رقم 15-04 المؤرخ في 01 فبراير سنة 2015[34]، وهو يعد أحد القوانين البارزة التي تهدف إلى تعزيز الثقة في المعاملات الإلكترونية وتوثيقها بشكل قانوني. في ظل التحول الرقمي الكبير الذي تشهده الجزائر والعالم، أصبحت المعاملات الإلكترونية جزءًا أساسيًا من الحياة اليومية، سواء كانت في قطاع الأعمال أو في القطاعات الحكومية. لذلك كان من الضروري أن يتم وضع إطار قانوني يضمن الاعتراف بالتوقيعات الإلكترونية على غرار التوقيعات التقليدية. ويهدف هذا القانون إلى تسهيل المعاملات الرقمية عبر الإنترنت، سواء كانت متعلقة بالبيع والشراء الإلكتروني أو بالتوقيع على الوثائق القانونية عن بُعد. بالإضافة إلى ذلك، يعزز هذا القانون من الأمان القانوني للأفراد والشركات ويمنع التزوير في الوثائق الرقمية.

ويشكل القانون رقم 18-04 المؤرخ في 10 مايو سنة 2018 [35] خطوة كبيرة نحو تنظيم البريد والاتصالات الإلكترونية في الجزائر. في هذا القانون، تم تحديد القواعد العامة المتعلقة بالبريد الإلكتروني والاتصالات عبر الإنترنت التي كانت تشهد توسعًا كبيرًا في الاستخدامات الشخصية والتجارية. وعُني القانون بتحديد أطر تنظيمية جديدة للقطاع وتطوير البنية التحتية لهذه الخدمات. هذا القانون يعكس تطور الجزائر في مجال تنظيم الاتصالات الإلكترونية من خلال إدخال تقنيات حديثة مثل الاتصالات الصوتية عبر الإنترنت وتوسيع نطاق خدمات الإنترنت عالي السرعة. كما تناول القانون كيفية تنظيم الخدمات المقدمة من مزودي الإنترنت وضمان الجودة والأسعار المناسبة للمستهلك، بالإضافة إلى توفير الحماية اللازمة للبيانات والمعلومات الشخصية للمستخدمين.

كما قام المشرع الجزائري باصدار القانون رقم 18-05 المؤرخ في 10 مايو سنة 2018[36] لتنظيم التجارة الإلكترونية في الجزائر في إطار سعي الحكومة الجزائرية لتطوير الاقتصاد

---

[33] - قانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009 وقد تم نشره في الجريدة الرسمية رقم 47 بتاريخ 25 شعبان 1430 الموافق 16 أغسطس 2009. يهدف الى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

[34] - القانون رقم 15-04 المؤرخ في 1 فبراير 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، نُشر في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية العدد 6 بتاريخ 11 ربيع الثاني عام 1436 الموافق لشهر فبراير سنة 2015

[35] - القانون رقم 18-04، المؤرخ في 24 شعبان عام 1439 الموافق 10 مايو سنة 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية .2تم نشر هذا القانون في الجريدة الرسمية رقم 27 بتاريخ 13 مايو 2018

[36] - القانون رقم 18-05، المؤرخ في 10 مايو 2018، يتعلق بالتجارة الإلكترونية .تم نشر هذا القانون في الجريدة الرسمية رقم 28 بتاريخ 16 ماي 2018

الرقمي. مع تزايد التجارة عبر الإنترنت في السنوات الأخيرة، حيث أصبح من الضروري وضع قوانين تنظم هذا النوع من التجارة. وجاء هذا القانون ليضمن تنظيم المعاملات الإلكترونية بما يتماشى مع المعايير الدولية. وقد حدد القانون كيفية إجراء المعاملات التجارية عبر الإنترنت من خلال تقنين عمليات البيع والشراء الرقمية، وضمان حماية حقوق المستهلك. بالإضافة إلى ذلك، تضمن هذا القانون إنشاء إطار قانوني للتجارة الإلكترونية الذي يساهم في تحفيز الشركات الجزائرية على استخدام هذه القنوات الحديثة للبيع والتسويق، مما يساهم في تعزيز الاقتصاد الوطني.

وفي ذات السنة صدر كذلك القانون رقم 18-07 المؤرخ في 10 يونيو سنة 2018 [37] المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وهو قانون ذو أهمية كبيرة في عصر تزايد جمع البيانات الشخصية واستخدامها في مختلف القطاعات. يعكس هذا القانون اهتمام الجزائر بحماية الخصوصية والبيانات الشخصية للمواطنين في العصر الرقمي. يتضمن هذا القانون مجموعة من الضوابط التي تهدف إلى تنظيم كيفية جمع البيانات الشخصية، واستخدامها، والاحتفاظ بها. كما يلزم الشركات والمؤسسات بتوفير حماية صارمة لهذه البيانات، ويحدد حقوق الأفراد في الاطلاع على بياناتهم الشخصية ومطالبة الشركات بحذفها أو تصحيحها عند الطلب. يعكس هذا القانون التزام الجزائر بمعايير حماية الخصوصية التي تحترمها الدول المتقدمة في مجال تشريعات البيانات.

وفي سنة 2020 صدر القانون رقم 20-04 المؤرخ في 30 مارس سنة 2020[38] المتعلق بتنظيم الاتصالات الراديوية في الجزائر، ويعتبر من أحدث القوانين التي تناولت تكنولوجيا الاتصالات في البلاد. مع التوسع الكبير في استخدام الإنترنت والاتصالات اللاسلكية، أصبح من الضروري تحديد القواعد الخاصة باستخدام الطيف الراديوي، وهو ما يعنى استخدام الموجات الكهرومغناطيسية لنقل البيانات عبر شبكات الاتصال. يتضمن القانون تنظيم استخدام الترددات الراديوية من قبل الشركات والمؤسسات الخاصة والعامة، وضمان تخصيص الترددات بشكل يتماشى مع احتياجات السوق. كما يحدد القانون صلاحيات سلطة الضبط في تنظيم توزيع هذه الترددات، ويتضمن معايير للأداء والنوعية في خدمات الاتصالات التي تعتمد على التقنيات الراديوية.

كما صدر **مؤخرا** القانون العضوي رقم 23-14 المتعلق بالإعلام[39] في الجزائر بهدف تنظيم مهنة الإعلام وضمان ممارستها بحرية وفقًا لأحكام الدستور، مع احترام الثوابت الوطنية والقيم الدينية والثقافية للأمة. وتضمن القانون 56 مادة تركز على ضمان حرية الإعلام وحماية حقوق الإنسان والحريات الفردية والجماعية، مع التأكيد على ضرورة أن تكون وسائل الإعلام مرتبطة برأس مال جزائري خالص، ويتم تحريرها بواسطة صحفيين محترفين. كما شدد القانون على منع تمويل وسائل الإعلام من جهات أجنبية للحفاظ على استقلالية الإعلام الوطني. وأنشأ القانون سلطة ضبط الصحافة المكتوبة والإلكترونية كسلطة مستقلة تهدف إلى تنظيم الإعلام المكتوب في

---

[37] - القانون رقم 18-07، المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، نُشر في الجريدة الرسمية رقم 34 بتاريخ 13 يونيو 2018.

[38] - القانون رقم 20-04 المؤرخ في 30 مارس سنة 2020 المتعلق بتنظيم الاتصالات الراديوية، ج ر ج ج 21 ابريل 2020

[39] - القانون العضوي رقم 23-14 المتعلق بالإعلام المؤرخ في 27 غشت 2023، ج ر ج ج عدد 77، تاريخ 02 ديسمبر 2023.

الجزائر، بالإضافة إلى سلطة وطنية مستقلة لضبط السمعي البصري، لتفعيل الرقابة وضمان الشفافية في القطاع الإعلامي.

كما أصدر المشرع الجزائري **القانون رقم 23-19** المتعلق بالصحافة المكتوبة والصحافة الإلكترونية في **2ديسمبر 2023**[40]، ويعد هذا القانون خطوة مهمة في تنظيم القطاع الإعلامي في الجزائر بشكل شامل. كما هدف هذا التشريع إلى تنظيم وتنمية الصحافة المكتوبة والإلكترونية، مع التركيز على تعزيز استقلالية وسائل الإعلام وحمايتها من التدخلات السياسية والاقتصادية. وحدد القانون أيضًا القواعد الخاصة بالمحتوى الإعلامي الذي يتم نشره عبر الصحافة المكتوبة والإلكترونية، مع وضع ضوابط تشجع على احترام حقوق الإنسان، وحماية الحياة الخاصة للأفراد، وتوفير مساحة لتعدد الآراء والاتجاهات. كما يُعزز القانون آليات الرقابة والتنظيم من خلال إنشاء هيئات مستقلة لضبط هذه الوسائل، مما يضمن التزام الصحف والمواقع الإلكترونية بالقوانين المعمول بها.

الفصل الثاني: تكنولوجيات الإعلام والاتصال ورقمنة الخدمات

شهدت الجزائر في السنوات الأخيرة توجهاً واضحاً نحو رقمنة الإدارة وتحديث الخدمات العمومية، وذلك ضمن سياسة وطنية تهدف إلى تحسين أداء المؤسسات العمومية، وتسهيل العلاقة بين الإدارة والمواطن من خلال إدماج تكنولوجيات الإعلام والاتصال. ويُعد هذا التحول الرقمي خياراً استراتيجياً لتحقيق الحوكمة، ومكافحة البيروقراطية، وتعزيز الشفافية والنجاعة الإدارية.

[40] - القانون رقم 23-19 المتعلق بالصحافة المكتوبة والصحافة الإلكترونية في 2ديسمبر 2023. ، ج ر ج ج عدد 77، تاريخ 02 ديسمبر 2023.

غير أن إنجاح هذا المسار يقتضي تجاوز مجموعة من التحديات ذات الطابع التقني، والمؤسسي، والتشريعي، إذ يتطلب الأمر وجود بنية تحتية تكنولوجية مؤمنة، وكفاءات بشرية مؤهلة، وأطر قانونية شاملة تواكب خصوصيات البيئة الرقمية وتحمي الحقوق الرقمية للمواطن.

من هذا المنطلق، تهدف هذه الدراسة إلى تحليل واقع رقمنة الخدمات في الجزائر من خلال رصد الجهود المبذولة لتفعيل تكنولوجيات الإعلام والاتصال في مختلف القطاعات، واستعراض أبرز التشريعات الوطنية ذات الصلة، إلى جانب الوقوف على العقبات التي لا تزال تعيق التحول الرقمي الشامل، واقتراح آليات لتجاوزها.

المبحث الأول: مفهوم رقمنة الخدمات وإدماج تكنولوجيات الإعلام والاتصال

في ظل التحولات المتسارعة التي يشهدها العالم بفعل التطورات التكنولوجية، باتت رقمنة الخدمات خيارًا استراتيجيًا تتبناه الدول من أجل تحقيق الفعالية في الأداء، والشفافية في المعاملات، وسهولة الوصول إلى المعلومة والخدمة. وقد ساهم إدماج تكنولوجيات الإعلام والاتصال في هذا التحول الرقمي بشكل جوهري، حيث أصبحت هذه التكنولوجيات حجر الأساس في عملية تحديث الأنظمة الإدارية والقانونية والاقتصادية. وتُعرّف تكنولوجيات الإعلام والاتصال بأنها الوسائل الرقمية التي تُستخدم في جمع ومعالجة وتخزين ونقل المعلومات، وتشمل الحواسيب، الإنترنت، الهواتف الذكية، الشبكات الرقمية، وأنظمة المعلومات. ومن خلال هذه الأدوات، أصبح من الممكن تطوير الخدمات العمومية، بما فيها خدمات العدالة، والتعليم، والصحة، وغيرها، لتُقدَّم بشكل أكثر سرعة وكفاءة.

وفيمايلي نتناول دراسة مفهوم رقمنة الخدمات في أبعاده التقنية والقانونية، وتسليط الضوء على آثارها وانعكاساتها على مستوى تقديم الخدمة وأهميتها .

المطلب الأول: التعريف برقمنة الخدمات

رقمنة الخدمات هي التحول من الأنظمة التقليدية المعتمدة على المعاملات الورقية إلى أنظمة إلكترونية تعتمد على تكنولوجيات الإعلام والاتصال لتقديم الخدمات للمواطنين بشكل أسرع وأكثر كفاءة. هذا التحول لا يشمل فقط رقمنة الإجراءات الإدارية، بل يتعداها إلى استخدام وسائل التكنولوجيا الحديثة مثل الحواسيب والإنترنت لتسهيل المعاملات بين الأفراد والإدارات، مما يساهم في تحسين تجربة المواطنين ويزيد من الشفافية والكفاءة.

في هذا السياق، تُعتبر الإدارة الإلكترونية جزءاً أساسياً من رقمنة الخدمات. تُعرّف الإدارة الإلكترونية بأنها "منظومة الأعمال والأنشطة التي يتم تنفيذها إلكترونيًا عبر الشبكات باستخدام النظم والوسائل الإلكترونية." [41].الهدف الرئيسي للإدارة الإلكترونية هو ميكنة كافة الأنشطة والمهام الإدارية بهدف تحسين الأداء الإداري، من خلال تقليل الاعتماد على الوثائق الورقية، تسريع الإجراءات، والتقليل من الروتين[42].. من خلال الإدارة الإلكترونية، يمكن تحقيق أهداف مثل

[41] - سعد غالب ياسين، الادارة الالكترونية، دار اليازوزي العلمية للنشر والتوزيع، الأردن، 2010، الطبعة الولى، ص 21.

[42] - عيسات عيني، التوجه نحو الادارة الالكترونية في الجزائر من خلال مشروع الجزائر الالكترونية 2013، ص84.

تنظيم المعاملات الحكومية، تحسين التواصل بين المواطن والإدارة، وتوفير وقت وجهد في إنجاز المعاملات.

بالتالي، فإن رقمنة الخدمات لا تقتصر على تقديم الخدمات الإلكترونية فحسب، بل تشمل تحسين الإدارة عبر الاستفادة من تكنولوجيات الإعلام والاتصال لتوفير خدمات أكثر فعالية وسرعة للمواطنين.

يعد إدخال تكنولوجيات الإعلام والاتصال في تسيير المرافق العمومية والخدمات الإدارية خطوة حاسمة نحو تحسين فعالية الأداء الحكومي وتعزيز كفاءة الإدارة العامة. من خلال استخدام هذه التكنولوجيا، يتم تحويل الخدمات التقليدية إلى منصات إلكترونية تسهم في تحسين التواصل بين الإدارات والمواطنين وتسهيل الإجراءات.

المطلب الثاني: الأهمية والأهداف الاستراتيجية لرقمنة الخدمات في الجزائر

تُعتبر رقمنة الخدمات في الجزائر خطوة هامة نحو تحقيق التحول الرقمي، وهو جزء من التوجه العالمي الذي يعتمد بشكل متزايد على تكنولوجيات الإعلام والاتصال في جميع المجالات. تتمثل أهمية هذا التحول في تحسين كفاءة وجودة الخدمات العامة، حيث يساهم في خلق بيئة أكثر شفافية وفاعلية.

من بين أهم الفوائد التي تحققها الرقمنة هو تعزيز الشفافية في العمل الإداري. إذ تتيح للموظفين والمواطنين متابعة سير المعاملات في الوقت الفعلي، مما يحد من البيروقراطية والفساد. كما تسهم الرقمنة في تحقيق العدالة في توزيع الخدمات، حيث تتيح لجميع المواطنين، بغض النظر عن أماكنهم أو أوضاعهم الاجتماعية، الوصول إلى الخدمات الحكومية بسهولة.

ومن من خلال إدخال تكنولوجيات الإعلام والاتصال في تسيير المرافق العامة، تسعى الحكومة الجزائرية إلى تحقيق عدة أهداف رئيسية، أبرزها:

- **تحسين الكفاءة الحكومية** :عبر استخدام الوسائل الرقمية، يمكن تسريع الإجراءات وتسهيل المعاملات، ما يقلل من الوقت والجهد على الجميع. وهذا يساعد على تقديم خدمات أسرع وأكثر دقة للمواطنين، في كافة القطاعات مثل التعليم والصحة والإدارة العامة.
- **مكافحة الفساد وتقليص البيروقراطية** :تعتبر الرقمنة وسيلة فعّالة لمحاربة الفساد الإداري، حيث تضمن الشفافية والمساءلة. بفضل النظام الرقمي، يمكن تتبع كافة المعاملات، مما يحد من التصرفات غير القانونية ويزيد من ثقة المواطنين في المؤسسات الحكومية.
- **تعزيز الاقتصاد الوطني** :تساهم رقمنة الخدمات في تحسين البيئة الاستثمارية في الجزائر. من خلال تبسيط الإجراءات الحكومية، تصبح الجزائر أكثر جذبًا للمستثمرين، مما يعزز الاقتصاد الوطني ويوفر فرص عمل جديدة.
- **تسهيل الوصول إلى الخدمات** :يمكن للرقمنة أن تضمن وصول جميع المواطنين إلى الخدمات الحكومية في أي وقت ومن أي مكان، ما يعزز **الإدماج الاجتماعي** ويضمن تساوي الفرص بين الجميع.

• **تحسين جودة الخدمات** :باستخدام التكنولوجيا، يمكن تحسين جودة الخدمات التي تقدمها الدولة للمواطنين، وهو ما يعزز من رضاهم ويقلل من عدد الشكاوى. التحول الرقمي يمكن أن يتيح تقديم خدمات أكثر كفاءة ودقة.

• **تشجيع الابتكار في القطاع العام** :الرقمنة توفر الفرصة للابتكار، حيث تفتح المجال لإنشاء تطبيقات وخدمات جديدة تتناسب مع احتياجات المواطنين، وتسمح بتقديم حلول مبتكرة وسريعة.
• **تحقيق التكامل بين القطاعات** :إدخال تكنولوجيات الإعلام والاتصال في مختلف القطاعات الحكومية يساهم في تعزيز التكامل بينها، مما يتيح تواصلاً أسرع وأكثر فاعلية بين قطاعات الصحة والتعليم والإدارة.
• **مواكبة التوجهات العالمية** :من خلال رقمنة الخدمات، تسعى الجزائر إلى مواكبة التطورات العالمية في مجال تكنولوجيا المعلومات والاتصالات، مما يعزز من مكانتها على الساحة الدولية ويفتح أبواب التعاون مع الدول الأخرى.

في النهاية، تهدف رقمنة الخدمات في الجزائر إلى تحويل طريقة تقديم الخدمات الحكومية لتصبح أكثر فاعلية وكفاءة، ما يسهم في تحسين حياة المواطنين وتعزيز النمو الاقتصادي والاجتماعي في البلاد.

المبحث الثاني: واقع تطبيق رقمنة الخدمات في الجزائر باستخدام تكنولوجيات الإعلام والاتصال

يشهد العالم في العصر الحديث تطورًا سريعًا في مجال تكنولوجيات الإعلام والاتصال، مما يساهم في تغيير أساليب العمل والإدارة في مختلف القطاعات. ولقد أصبح اعتماد الرقمنة أحد المحاور الأساسية لتحسين أداء الخدمات في الدول الحديثة، بما في ذلك الجزائر. ومع هذا التحول الرقمي، تتعدد التحديات التي تواجه الجزائر في تطبيق هذه التكنولوجيا في مختلف المجالات.

وتتمثل التطبيقات الأساسية لتكنولوجيا الإعلام والاتصال في القطاعات الحيوية مثل التعليم، الصحة، والإدارة العامة، مما يُظهر الأثر الكبير لهذه التكنولوجيا في تحسين وتطوير الخدمات العامة. إلا أن هناك العديد من التحديات التي قد تعيق انتشار الرقمنة، سواء كانت تحديات تقنية أو تنظيمية أو حتى ثقافية، وهو ما يستدعي دراسة الأسباب الكامنة وراء تلك الصعوبات.

ومن أجل تحقيق نجاح عملية الرقمنة في الجزائر، يجب العمل على تحقيق متطلبات أساسية عدة، مثل تطوير البنية التحتية الرقمية، وتعزيز المهارات التقنية، ووضع سياسات تشريعية تواكب التحولات الرقمية. لا بد من التأكيد على أن تجاوز هذه التحديات يتطلب استراتيجية محكمة ومتطلبات واضحة لضمان فعالية الرقمنة في تحسين الخدمات العامة.

ويتناول هذا المبحث واقع تطبيق رقمنة الخدمات في الجزائر باستخدام تكنولوجيات الإعلام والاتصال من خلال تسليط الضوء على التطبيقات الحالية لهذه التكنولوجيا في القطاعات الحيوية، التحديات التي تواجهها، والمتطلبات الأساسية التي يجب تحقيقها لضمان نجاح عملية الرقمنة.

المطلب الأول: واقع تطبيقات الرقمنة في القطاعات الحيوية بالجزائر

سعت الجزائر منذ عام 2013 إلى تحقيق تحول رقمي شامل من خلال مشروع "الجزائر الإلكترونية"، وهو مبادرة تهدف إلى تفعيل تكنولوجيا المعلومات والاتصالات في العديد من القطاعات الحيوية مثل الإدارة العامة، الاتصالات، البنوك، وغيرها. هذا المشروع لا يزال مستمراً ويحقق تقدماً في تطبيق الرقمنة عبر مختلف المجالات. في هذا السياق، نعرض فيما يلي بعض الأمثلة البارزة لتطبيقات الرقمنة في القطاعات الأساسية:

أولاً: رقمنة مصلحة الحالة المدنية

يعد مشروع رقمنة مصلحة الحالة المدنية أحد أبرز مظاهر تحول الجزائر الرقمي. فقد تم إنشاء السجل الوطني الآلي للحالة المدنية تحت إشراف وزارة الداخلية، بموجب القانون رقم 14-08[43] الذي تم تعديله ليشمل جميع عقود الحالة المدنية مثل المواليد، الوفيات، والزواج في مختلف البلديات الجزائرية. هدف هذا المشروع هو تمكين المواطنين من استخراج وثائق الحالة المدنية بشكل فوري من أي بلدية أو ملحق إداري دون الحاجة للتنقل.

في هذا الإطار، أُصدر المرسوم التنفيذي رقم 15-315[44]، الذي يسمح بإصدار نسخ إلكترونية من وثائق الحالة المدنية. هذه الوثائق تُمهَر بتوقيع إلكتروني موصوف، مما يضمن أن الوثائق المرسلة عبر الإنترنت تتمتع بنفس مصداقية الوثائق الأصلية وفقاً للتشريعات الجزائرية.

وضمن جهود الحكومة لتحسين خدمات المواطنين، تم إدخال جواز السفر البيومتري بداية من 5 يناير 2012، وهو التغيير الذي تم بموجب القرار المؤرخ في 26 ديسمبر 2011[45]. تم استبدال الجوازات التقليدية بجوازات السفر البيومترية، مع استمرارية العمل بالجوازات القديمة حتى سحبها نهائيًا. تم منح صلاحية إصدار جواز السفر البيومتري للدوائر المحلية فقط، على أن يتم تعميم الخدمة على مستوى البلديات في مارس 2015.

وفي إطار تحديث البنية الرقمية للإدارة العامة، تم تعديل قانون الحالة المدنية بموجب القانون رقم 17-03[46]، حيث تم إدخال بطاقة التعريف الوطنية البيومترية الإلكترونية. هذا التعديل أتاح إصدار بطاقة جديدة تحتوي على شريحة إلكترونية لزيادة الأمان. يتم إعداد هذه البطاقة على مستوى البلديات وفقاً للتنظيم الجديد، كما تم تحديد كيفية تجديدها. كما انه في اطار التحول الرقمي في مصلحة النقل، تم إصدار رخص القيادة البيومترية في الجزائر بدءًا من 1 أبريل 2018. تم تنفيذ هذا المشروع بموجب منشور وزاري مشترك بتاريخ 4 يونيو 2018، مع تخصيص الرقابة والإشراف من قبل وزارة الداخلية والجماعات المحلية. تم تعميم إصدار رخص القيادة البيومترية أولاً على أربع بلديات في الجزائر العاصمة في يونيو من نفس السنة، لتُستكمل عملية التعميم على جميع بلديات البلاد بنهاية 2018.

---

[43] - القانون رقم 14-08 المتضمن تعديل قانون الحالة المدنية رقم 70-20 ، المؤرخ في 09 أوت 2014، ج ر ج ج، عدد 49، تاريخ النشر 20 أوت 2014.

[44] - المرسوم التنفيذي رقم 15-3015، المتعلق بإصدار نسخ وثائق الحالة المدنية بطريقة الكترونية، المؤرخ في 10 ديسمبر 2015، ج ر ج ج عدد68 ، الصادرة بتاريخ 27 ديسمبر 2015.

[45] - القرار المؤرخ في 26 ديسمبر 2011 المحدد لتاريخ تداول جواز السفر الوطني البيومتري الالكتروني، ج ر ج ج، عدد01، تاريخ 14 جانفي 2011.

[46] - القانون رقم 17-03 المتضمن تعديل قانون الحالة المدنية ، الصادر بتاريخ 2017/01/10، ج ر ج ج عدد 02، تاريخ 2017/01/11.

ثانيًا: رقمنة خدمات مؤسسة البريد والمواصلات

عملت مؤسسة البريد والمواصلات على تطوير وتحسين خدماتها من خلال دمج تكنولوجيا المعلومات والاتصال في مختلف أنشطتها، وذلك بهدف تسهيل الوصول إلى الخدمات المالية والإدارية[47]. من بين هذه الخدمات، تم توفير أجهزة سحب الأموال الآلي التي تتيح للمواطنين إجراء عمليات سحب نقدي بمبالغ محددة، وذلك في أي وقت من اليوم، مع القدرة على تكرار العملية وفق الحاجة. إضافة إلى ذلك، تم إطلاق بطاقات السحب الإلكتروني التي تتيح للمواطنين الحصول على خدمات مالية بسهولة. يمكن لحاملي هذه البطاقات سحب الأموال من أي جهاز صراف آلي متوفر في الجزائر، مما يعزز مرونة الوصول إلى الخدمات المصرفية.

كما تتيح مؤسسة بريد الجزائر للمواطنين العديد من الخدمات الإلكترونية عبر الإنترنت، مثل التحقق من الرصيد، طلب صك بريدي، والحصول على كشوفات الحسابات المالية. هذه الخدمات تُسهم في تسهيل العمليات المصرفية وتوفير الوقت والجهد. ومن بين أبرز المبادرات التي أطلقتها المؤسسة هي "البطاقة الذهبية" التي توفر لحاملها إمكانية إجراء العديد من المعاملات المالية، مثل سحب الأموال من أجهزة الصراف الآلي المنتشرة في مراكز البريد أو في البنوك الأخرى. كما يمكن استخدامها في تسديد المشتريات من المؤسسات التجارية التي تقبل الدفع عبر هذه البطاقة، بالإضافة إلى إمكانية دفع فواتير المياه والكهرباء عبر المكتب البريدي الافتراضي على الإنترنت. وتدعم البطاقة أيضًا الشراء عبر الإنترنت من المواقع التي تقبل الدفع ببطاقاتCIB ، مثل شركات الهاتف النقال ومؤسسة الخطوط الجوية الجزائرية، مما يعزز من تنوع الخدمات المتاحة للمواطنين عبر الأنظمة الإلكترونية[48].

ثالثا: رقمنة خدمات قطاع العدالة :

تعتبر الرقمنة في القطاع القضائي في الجزائر جزءًا محوريًا من الإصلاحات الشاملة التي تهدف إلى تحديث النظام القضائي وتعزيز الشفافية والفعالية. من خلال استخدام التقنيات الحديثة، يمكن تحسين عمليات إدارة الملفات القضائية، وتسهيل الوصول إلى المعلومات، وتعزيز التواصل بين الجهات المعنية. تشمل جهود الرقمنة تطبيقات متنوعة، مثل الأنظمة الإلكترونية لإدارة المحاكم وتسجيل القضايا، تقنيات التعرف الضوئي على الحروف لتسريع معالجة الوثائق، وكذلك الأنظمة الإلكترونية لمراقبة الإجراءات القضائية[49] .

تسهم هذه المبادرات في تحسين كفاءة العدالة وتعزيز ثقة المواطنين في النظام القضائي، كما تساهم في تقليص الازدحام في المحاكم وتقليل الاعتماد على الإجراءات الورقية. هذا التحول يؤدي في نهاية المطاف إلى تحقيق العدالة بشكل أسرع وأكثر شمولًا. بلا شك، يمثل التحول الرقمي في

---

[47] - بريد الجزائر: ماضٍ في الانتقال نحو الرقمنة .جريدة الرائد، 10 أكتوبر 2023 .الرابط. https://elraed.dz/158581

[48] - يحياوي، الهام" .دور الرقمنة في ترقية الخدمة العمومية بالجزائر: البطاقة الذهبية نموذجا ".مجلة التحليل والاستشراف الاقتصادي، المجلد 3، العدد 1، 2022، ص. 63-80.

[49] - بياوي جلال ، التحول الرقمي في القطاع القضائي تحول العدالة في العصر الرقمي: جريدة البديل ، 06افريل 2025، الساعة 16:00 على الموقع التالي: elbadilabc-ar.dz/?p=30853

القطاع القضائي تحديًا وفرصة في آن واحد. بجانب تحسين كفاءة العدالة وتسريع الإجراءات القانونية، تساهم الرقمنة أيضًا في تعزيز حقوق المواطنين وضمان وصول عادل إلى العدالة.[50].

وفي سبيل ذلك أنشأت وزارة العدل الجزائرية هيئة مختصة تحت مسمى "المديرية العامة لعصرنة العدالة"، تهدف إلى تنفيذ برنامج الإصلاح الرامي إلى تسهيل الوصول إلى العدالة للمواطنين بشكل أكثر فاعلية وسرعة. تقوم هذه الهيئة بتوفير كافة الأدوات التكنولوجية اللازمة للقضاة والفاعلين في القطاع القضائي، بما في ذلك المحامون والمحضرون، لضمان إنجاز مهامهم بأعلى مستوى من الكفاءة.

في الجانب التشريعي، أطلق المشرع الجزائري مجموعة من القوانين والأنظمة التي تهدف إلى تحديث قطاع العدالة وتحسين خدماته، أبرزها القانون رقم 15-03 المتعلق بعصرنة العدالة[51]. هذا القانون نظم المنظومة المعلوماتية المركزية لوزارة العدل، وعمل على توثيق صحة الوثائق الإلكترونية وتفعيل التصديق الإلكتروني للمستندات والمحررات القضائية التي تصدرها وزارة العدل والمؤسسات التابعة لها. كما نظم طريقة إرسال الوثائق والإجراءات القضائية عبر الإنترنت، وحدد شروط استخدام المحادثات المرئية عن بعد في الإجراءات القضائية، مما يسهل التواصل بين الأطراف عند الحاجة لتقليص المسافات أو ضمان سير العدالة بسلاسة.

ووفقاً لهذا القانون، تم اعتماد نظام المحاكمة عن بعد باستخدام شبكة الألياف البصرية التي تربط جميع الجهات القضائية والمؤسسات العقابية على امتداد التراب الوطني. هذا النظام يتيح إجراء المحاكمات والتواصل مع الأطراف والشهود والخبراء الذين قد يتواجدون في أماكن بعيدة، مما يسهم في تقليص أعباء التنقل وتأجيل القضايا بسبب غياب الشهود[52]..

كما أطلق المشرع آلية الرقابة الإلكترونية كبديل للحبس المؤقت بموجب الأمر رقم 15-02 لعام 2015، الذي يعدل ويكمل قانون الإجراءات الجزائية. ويستند هذا النظام إلى استخدام سوار إلكتروني يتم وضعه على معصم المتهم طوال فترة خضوعه للرقابة، مما يتيح تحديد موقعه وتوقيت وجوده.

وفي خطوة أخرى لتعزيز الرقمنة في القطاع القضائي، أنشأت وزارة العدل في سبتمبر 2014 مركزاً خاصاً لإصدار شرائح التوقيع الإلكتروني، حيث يتم تزويد القضاة والنواب العامين وأمناء الضبط بهذه الشرائح التي تحمل توقيعاتهم الإلكترونية الخاصة، مما يسهل تبادل الوثائق الإلكترونية بينهم عبر مختلف الجهات القضائية في أنحاء البلاد.

منذ نوفمبر 2003، تم تزويد قطاع العدالة في الجزائر بموقع إلكتروني خاص هو www.mjustice.dz، الذي خصص لإعلام المواطنين بكل أنشطة وزارة العدل وتنظيم القطاع

---

[50] - بوعرقوب نعمة، سوداني أحلام، "رقمنة الخدمة العمومية بقطاع العدالة في الجزائر: المكاسب والتحديات"، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد 1، 21 جانفي 2024، الصفحات 659–684.

[51] - القانون رقم 03-15 المتعلق بعصرنة العدالة الصادر في 01 فبراير 2015 ، ج ر ج الجزائرية العدد 06، تاريخ النشر 2015/02/10.

[52] - وقد تمت أول محاكمة عن بعد داخل الوطن بتاريخ 2015/10/07 بمحكمة القليعة، وأخرى دولية بتاريخ 2016/07/11 بمجلس قضاء المسيلة وفيها تم التحدث مع الشاهد بتقنية الصوت والصورة الحاضر في مجلس قضاء "نانتير" الفرنسي سالم بركاهم ,بواشري أمينة ، الاصلاح الاداري في الجزائر عض تجرة مرفق العدالة (1999-2017) المجلد 06، العدد 01، 2018. ص 225

وخدماته المقدمة للجمهور. يهدف الموقع إلى تسهيل الاطلاع على القواعد القانونية وأحدث المستجدات القانونية للمواطنين والوافدين على حد سواء. بالإضافة إلى ذلك، تم إنشاء مواقع إلكترونية خاصة بالجهات القضائية المختلفة والمصالح التابعة لوزارة العدل، حيث توفر هذه المواقع معلومات حول نشاطاتها وتسمح بالتواصل مع هذه الجهات عبر البريد الإلكتروني الخاص بكل منها.

كما تم تحسين التنظيم التشريعي لجريدة الرسمية الجزائرية عبر الموقع www.joradp.dz، الذي تم تزويده بمحرك بحث تلقائي، مع إمكانية تنزيل ونسخ التشريعات والقوانين الجزائرية مباشرة من الموقع. وقد تم إضافة خدمة جديدة على الموقع الرسمي لوزارة العدل للإجابة على استفسارات المواطنين، حيث يتم استقبال الاقتراحات والشكاوى والرد عليها أو توجيهها إلى الهيئات المختصة في وقت قياسي[53]. وفي إطار تحسين الخدمات الإلكترونية، أصبح بإمكان المواطن الجزائري استخراج البطاقة رقم 03 من صحيفة السوابق القضائية من أي محكمة عبر التراب الوطني وفي وقت قياسي، بغض النظر عن مكان بلدية ميلاده. كما يمكنه سحب هذه البطاقة عبر الإنترنت من خلال الموقع الإلكتروني لوزارة العدل[54]، وذلك لكل جزائري أو أجنبي مقيم بالجزائر بشرط أن تكون صحيفته خالية من أي عقوبة، وقد تم توفير هذه الخدمة أيضاً للجالية الجزائرية في الخارج.

ومنذ عام 2010، أصبح بإمكان المتقاضين متابعة مآل قضاياهم عبر موقع وزارة العدل، مما يسهل المتابعة الآلية للملفات القضائية في جميع الجهات القضائية المنتشرة عبر التراب الوطني. كما تم توفير خدمة سحب النسخة العادية للقرارات الصادرة عن المحكمة العليا ومجلس الدولة موقعة إلكترونياً، دون الحاجة إلى التوجه شخصياً إلى مقر الجهة القضائية المصدرة لها.

تتبنى الجزائر أيضاً نظاماً إلكترونيًا متطورًا لإدارة ومتابعة المحبوسين، والذي يعد جزءًا مهمًا من عملية إعادة إدماجهم. يسمح هذا النظام بمتابعة وضعيات السجناء وتوزيعهم وفقًا لدرجة خطورتهم، بالإضافة إلى تتبع مسار كل سجين منذ دخوله إلى السجن وتوثيق أسباب ذلك وسلوكه خلال فترة احتجازه. يتم تطبيق هذا النظام في جميع المؤسسات العقابية على مستوى التراب الوطني، مما يعزز القدرة على مراقبة وإدارة عملية إعادة الإدماج.

كما قامت وزارة العدل الجزائرية بتوفير أرضية إلكترونية جديدة تتيح للأفراد سواء كانوا طبيعيين أو معنويين (إدارات، مؤسسات، شركات خاصة، جمعيات) تقديم الشكاوى أو العرائض عن بعد، مما يمثل خطوة هامة نحو تفعيل آلية رفع الدعوى إلكترونيًا في المجال الجنائي فقط، حيث تُرفع الشكوى أمام النيابة العامة. للاستفادة من هذه الخدمة، يتعين على مقدم الشكوى الدخول إلى منصة "النيابة الإلكترونية" عبر البوابة الإلكترونية لوزارة العدل، حيث يقوم بتعبئة استمارة تحتوي على معلوماته الشخصية، عنوانه، رقم هاتفه المحمول، وتحديد نوع الشكوى/العريضة ومضمونها. يتم تحويل الشكوى بشكل آلي إلى ممثل النيابة (وكيل الجمهورية أو النائب العام)

---

[53] - فاتح، مزيتي، مظاهر رقمنة مرفق العدالة وأثرها على تحسين الخدمة العمومية للمتقاضين، مجلة بيبليوفيليا لدراسات المكتبات والمعلومات ، المجلد 01، العدد 04، (2019). ص 20.

[54] - وكالة الأنباء الجزائرية: رقمنة قطاع العدالة : سحب قرابة مليوني صحيفة سوابق قضائية عن بعد خلال سنة 2022 أدرج يوم : الجمعة, 02 جوان 2023 18:30:
https://www.aps.dz/ar/algerie/144818-2022

لاتخاذ الإجراء المناسب، ويُعلم المعني بمآل شكواه والإجراءات المتخذة عبر المنصة الإلكترونية أو من خلال رسالة نصية قصيرة (SMS) أو البريد الإلكتروني.

وفي خطوة إضافية لضمان استمرارية الخدمات الإلكترونية لقطاع العدالة، تم إنشاء مركز بيانات احتياطي في القليعة بتاريخ 3 مايو 2015. يتيح هذا المركز استمرارية العمل في حال حدوث أي طارئ يؤثر على المركز الرئيسي في الأبيار، مثل الكوارث الطبيعية أو الأعمال التخريبية. يتم تشغيل المركز الاحتياطي وفقًا للمعايير الدولية لضمان استمرارية العمل الفورية، مما يسمح بإعادة تشغيل جميع الأنظمة فورًا للحفاظ على سير العمليات بشكل سلس وآمن.

كما تم استحداث مصلحة مركزية للبصمات الوراثية، يديرها قاض وتساعده خلية تقنية، تشرف على عملية إنشاء وإدارة قاعدة المعطيات الوطنية للبصمات الوراثية، وفقا لأحكام القانون رقم 16-03، المؤرخ في 19 جوان 2016 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص، وذلك لضمان الحماية القانونية للمعطيات الوراثية المحفوظة على مستواها[55].

رابعا : رقمنة قطاع التعليم العالي في الجزائر:

شهد قطاع التعليم العالي والبحث العلمي في الجزائر خطوات متقدمة نحو الرقمنة، تجسدت من خلال إطلاق مجموعة من المنصات الرقمية التي تهدف إلى تحسين جودة التعليم وتيسير الخدمات الجامعية[56]. من أبرز هذه المبادرات:

- **نظام "البرُوغْرَس :(Progres)** "وهو منصة رقمية وطنية متكاملة، تُعنى بمتابعة المسار الأكاديمي للطلبة في مختلف الأطوار الجامعية (الليسانس، الماستر، والدكتوراه)، كما تُستخدم في تسيير الخدمات الجامعية كالإيواء والمنح. وتمتد وظائف النظام أيضًا إلى تسيير المسار المهني والبيداغوجي للأساتذة الجامعيين، مما يُسهم في تعزيز الشفافية والفعالية الإدارية.
- **النظام الوطني للتوثيق عبر الخط :(SNDL)** أنشأه مركز البحث في الإعلام العلمي والتقني(CERIST) ، ويُعنى برقمنة الرسائل الجامعية (ماجستير، دكتوراه) وإتاحتها للبحث والاطلاع إلكترونيًا، ما يدعم الباحثين في الوصول السريع إلى المعرفة الأكاديمية.
- **المنصة الجزائرية للمجلات العلمية :(ASJP)** وهي أرضية رقمية متخصصة في نشر البحوث العلمية في مختلف التخصصات، تُدار تقنيًا من مركزCERIST ، بينما يُشرف على محتواها العلمي رؤساء تحرير المجلات الجامعية.
- **المنصة البيداغوجية التفاعلية :(Moodle)** تُعد فضاءً تعليميا رقميا يجمع بين الأستاذ والطالب، حيث يقوم الأستاذ بنشر محاضراته والأعمال التطبيقية الخاصة بالمقياس المكلف به، مع إمكانية التفاعل من خلال الأسئلة والملاحظات، مما يُعزز من جودة التعليم عن بعد.
- **البريد المهني المؤسسي :**وهو وسيلة رقمية رسمية تتيح التواصل بين مؤسسات التعليم العالي فيما بينها وبين الوزارة الوصية، كما يُستخدم في التواصل الإداري بين الإدارة والأساتذة، ويوفر أيضًا قناة اتصال بين الأساتذة والطلبة في إطار المتابعة البيداغوجية.

---

[55] - موقع وزارة العدل الجزائرية ، تاريخ الاطلاع 2025/04/06 :
https://www.mjustice.dz/ar/modernisation-2-2-2/

[56] - بريزة بوزعيب، الرقمنة ودورها في عصرنة التعليم العالي في الجزائر، مجلة جودة الخدمة العمومية للدراسات السيسيولوجية والتنمية الادارية، المجلد 05، العدد02، 2022، ص 75.

خامسا: رقمنة قطاع الضمان الاجتماعي في الجزائر:

في إطار سعيها لتحديث منظومة الحماية الاجتماعية ومواكبة التطورات التكنولوجية، عملت الجزائر على رقمنة قطاع الضمان الاجتماعي من خلال تبني آليات رقمية جديدة تهدف إلى تحسين فعالية الأداء وتقليص البيروقراطية. ولعل من أبرز هذه المبادرات إطلاق بطاقة الشفاء الإلكترونية، التي تمثل نقلة نوعية نحو تسيير عصري وشفاف لمختلف خدمات التأمين والتعويض الاجتماعي.

تُعد بطاقة الشفاء أداة رقمية ذكية تُستخدم لحفظ بيانات المؤمن لهم اجتماعيًا، وقد مكّنت من تجاوز العديد من العراقيل التقليدية التي كانت تعيق سير التعويضات والخدمات، مثل بطء الإجراءات وتعقيد المعاملات الإدارية. وقد تم الشروع في هذا المشروع سنة 2007 من خلال إنشاء مركز شخصنة البطاقات، ليتم بعدها تعميم العمل بها على المستوى الوطني في سنة 2011، حيث شملت جميع فئات المؤمنين اجتماعيا ومختلف ولايات الوطن.

أما من الناحية القانونية، فقد تم تأطير المشروع من خلال إصدار القانون 08-01 المؤرخ في 23 جانفي 2008، المعدل والمتمم للقانون 83-11 المؤرخ في 2 جويلية 1983 المتعلق بالتأمينات الاجتماعية، بالإضافة إلى المرسوم التنفيذي رقم 10-136 المؤرخ في 18 أفريل 2010، الذي حدد محتوى البطاقة الإلكترونية وشروط تسليمها، وكذا المفاتيح الإلكترونية المعتمدة لدى هياكل العلاج ومهنيي الصحة[57]..

المطلب الثاني: التحديات والعوائق أمام رقمنة الخدمات في الجزائر

رغم الجهود المبذولة من قبل السلطات الجزائرية في دفع عملية التحول الرقمي بمختلف القطاعات، إلا أن هذه العملية لا تزال تواجه مجموعة من التحديات والعوائق التي تعرقل مسارها وتؤثر على مدى فعاليتها واستمراريتها. ويمكن تلخيص أبرز هذه التحديات فيما يلي:

أولًا: ضعف البنية التحتية التكنولوجية : تُعدّ البنية التحتية الرقمية في الجزائر، خصوصًا في المناطق الريفية والنائية، من أبرز العوائق التي تعيق تقدم الرقمنة. لا تزال تغطية الإنترنت ضعيفة في بعض الولايات، حيث تعتمد بعض المناطق فقط على شبكات الجيل الثالث (3G)، ما يؤثر سلبًا على إمكانية النفاذ المتكافئ إلى الخدمات الرقمية، سواء من قبل المواطنين أو المؤسسات.

ثانيًا: نقص المهارات والكفاءات الرقمية: تواجه الجزائر عجزًا واضحًا في الكفاءات البشرية المؤهلة لإدارة وتشغيل المنصات الرقمية بكفاءة. كما يفتقر العديد من المواطنين إلى المهارات التقنية اللازمة لاستخدام الخدمات الإلكترونية، مما يستدعي تفعيل برامج وطنية لتكوين الموارد البشرية في المجال الرقمي، وتعزيز الثقافة التكنولوجية في المجتمع.

ثالثًا: غياب الإطار القانوني المتكامل: لا تزال التشريعات الجزائرية الخاصة بالرقمنة مشتتة أو غير كافية، الأمر الذي يخلق فجوات قانونية تعيق اعتماد الأنظمة الرقمية وتحد من ثقة

[57] - عرابة الحاج، زرقون محمد، عصرنة نظام الضمان الاجتماعي في الجزائر، تجربة بطاقة الشفاء، مجلة الباحث الاقتصادي، العدد02، 2014، ص 127.

المواطنين فيها. هناك حاجة ملحة إلى سن قوانين واضحة تنظم استخدام البيانات الإلكترونية، وتضبط آليات حماية الخصوصية والشفافية في تقديم الخدمات الرقمية.

رابعًا: ضعف الأمن السيبراني: إن تصاعد التهديدات الإلكترونية، في ظل توسع استعمال الأنظمة الرقمية، يفرض ضرورة وضع استراتيجيات متقدمة للأمن السيبراني. وقد أظهرت تجارب رقمية سابقة هشاشة البنى الرقمية أمام محاولات الاختراق، ما يتطلب تدعيم أنظمة الحماية وتكوين فرق مختصة في أمن المعلومات.

خامسًا: مقاومة التغيير وضعف الثقافة الرقمية: يشكل غياب الوعي بأهمية الرقمنة، لا سيما داخل المؤسسات الإدارية، عائقًا كبيرًا أمام التحول الرقمي. فبعض الهياكل ما زالت تعتمد الأساليب التقليدية وتقاوم الانتقال إلى البيئة الرقمية، في ظل غياب الحوافز والتكوين اللازم لمرافقة هذا التغيير.

سادسًا: نقص التمويل والدعم الفني: تواجه العديد من المؤسسات، خاصة الصغيرة والمتوسطة، صعوبات في تمويل مشاريع الرقمنة وتوظيف الكفاءات الفنية المؤهلة. كما تعاني من نقص في الإمكانيات التكنولوجية، ما يحدّ من قدرتها على المساهمة في المنظومة الرقمية الوطنية.

سابعًا: تحديات تطبيقية في القطاعات الحيوية : رغم إطلاق عدد من المشاريع الرقمية في قطاعات التعليم العالي، والضمان الاجتماعي، والعدالة، إلا أن التطبيق العملي لا يزال يواجه عقبات تتعلق بعدم تكامل المنصات، وبطء التفاعل، وانعدام الربط البيني بين الأنظمة المختلفة، ما يضعف من فعالية هذه الحلول الرقمية.

المطلب الثالث: المتطلبات الأساسية لإنجاح عملية الرقمنة في الجزائر

إن التحول الرقمي في الجزائر لا يمكن أن يحقق أهدافه المنشودة ما لم يُدعّم بجملة من الشروط والمتطلبات الأساسية التي تضمن استمراريته وفعاليته. فعملية الرقمنة ليست مجرد استحداث منصات إلكترونية أو رقمنة بعض الإجراءات، بل هي مشروع إصلاحي شامل يتطلب بيئة متكاملة تتوفر فيها مقومات النجاح. ومن أبرز هذه المتطلبات:

أولًا: تطوير البنية التحتية الرقمية: يُعدّ تعزيز شبكات الاتصال وتوفير تجهيزات الإعلام الآلي الحديثة في مختلف القطاعات، خاصة في المناطق النائية، من الركائز الأساسية لأي عملية رقمنة ناجحة. ويشمل ذلك توسيع نطاق تغطية الإنترنت وتحسين جودته لضمان نفاذ الجميع إلى الخدمات الرقمية.

ثانيًا: توفير الموارد البشرية المؤهلة: إن تأهيل الكفاءات البشرية وتدريبها على استخدام الأدوات الرقمية الحديثة يُعد من الشروط الجوهرية للرقمنة. فنجاح التحول الرقمي يتطلب موظفين متمكنين من المهارات التكنولوجية، قادرين على إدارة المنصات الرقمية وتطويرها باستمرار.

ثالثًا: تأمين الفضاء السيبراني: يتطلب إنجاح الرقمنة تعزيز نظم الأمن السيبراني لحماية البيانات والمعاملات الإلكترونية من القرصنة والتجسس والتسريبات. ويشمل ذلك تبني سياسات صارمة في مجال حماية المعلومات وتحديث الأنظمة الأمنية بصفة دورية.

رابعًا: تحديث الإطار التشريعي والتنظيمي: من الضروري ملاءمة المنظومة القانونية مع البيئة الرقمية الحديثة، وذلك من خلال سن قوانين تُنظم التعاملات الإلكترونية، وتضبط مسؤوليات الأطراف، وتحمي حقوق المتعاملين الرقميين، خاصة فيما يتعلق بالمعاملات الإدارية والتجارية والقضائية.

خامسًا: نشر الثقافة الرقمية وتحسيس المواطن: لا يمكن للرقمنة أن تحقق آثارها الفعلية ما لم يتم توعية المواطن بجدواها وأهميتها في تسهيل الحصول على الخدمات. ويُعدّ التحسيس والتكوين المستمر للمواطنين حول كيفية استخدام الخدمات الإلكترونية خطوة ضرورية لضمان انخراطهم الفعلي في المنظومة الرقمية.

الفصل الثالث: تكنولوجيات الإعلام والاتصال في المجال القانوني والقضائي

في العصر الرقمي الذي نعيشه اليوم، أصبح لتكنولوجيا الإعلام والاتصال تأثير كبير على مختلف المجالات، ومن أبرزها المجال القانوني والقضائي. لقد جلبت هذه التكنولوجيات ثورة حقيقية في الطريقة التي تُدار بها القضايا والإجراءات القانونية، إذ أصبحت تساهم بشكل رئيسي في تسريع وتسهيل العملية القضائية. لم تقتصر هذه التكنولوجيا على تحسين الآليات القانونية فقط، بل شملت أيضًا تحديث أساليب الإثبات القانوني، سواء في القضايا المدنية أو الجنائية.

في هذا الفصل، سنتناول كيف أثرت هذه التكنولوجيات على الإثبات القانوني، من خلال استخدام الأدوات الحديثة مثل الإثبات الإلكتروني، التصديق الإلكتروني، وحفظ الوثائق إلكترونيًا. كما سنتطرق إلى التحديات التي يواجهها النظام القضائي في قبول الأدلة الرقمية، وكيفية تكيف القضاة مع هذه التطورات التكنولوجية. ما يميز هذا التحول هو أن الإجراءات القانونية أصبحت أكثر سرعة وكفاءة، مع تعزيز الشفافية وتقليل التكاليف، مما يساهم في بناء الثقة في النظام القضائي ويجعل الوصول إلى العدالة أكثر سهولة.

المبحث الأول: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني

الإثبات القانوني هو الأساس الذي يبنى عليه قرار القاضي في أي قضية، حيث يعكس حقيقة الوقائع ويوضح الأطراف المتنازعة. ومع دخول تكنولوجيا الإعلام والاتصال إلى مجال الإثبات، أصبح لدينا أدوات جديدة تساهم في تقديم أدلة أكثر دقة ووضوحًا. الإثبات الإلكتروني على وجه الخصوص أصبح يشكل جزءًا كبيرًا من الدليل القانوني، حيث يتيح للأطراف تقديم الأدلة بطريقة رقمية آمنة وسريعة، مما يعزز من مصداقية الوثائق والمستندات.

بالإضافة إلى ذلك، أصبح التصديق الإلكتروني جزءًا أساسيًا في عملية التأكد من صحة الأدلة الرقمية، مما يساعد في ضمان أن الوثائق الإلكترونية التي تقدم في المحكمة لم يتم التلاعب بها أو تزويرها. ومن ناحية أخرى، قدمت تكنولوجيا الحفظ الإلكتروني للوثائق حلاً فعالًا للحفاظ على الأدلة لفترات طويلة، حيث أصبح من الممكن تخزين المستندات بشكل آمن بحيث يمكن الوصول إليها بسهولة عند الحاجة.

لكن مع هذه الفوائد، تظل هناك تحديات قانونية وتقنية يجب التغلب عليها، خاصة فيما يتعلق بكيفية قبول هذه الأدلة الإلكترونية في المحاكم. لابد من وضع آليات قانونية واضحة تضمن حقوق الأطراف وتحمى الأدلة من التلاعب. في هذا المبحث، سنستعرض تأثير تكنولوجيات الإعلام والاتصال على الإثبات القانوني في القضايا المدنية والجنائية، بالإضافة إلى التحديات التي تواجه المحاكم في قبول الأدلة الرقمية وكيفية التعامل معها بما يتماشى مع المعايير القانونية.

المطلب الأول: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني المدني

أثرت تكنولوجيات الإعلام والاتصال بشكل كبير على أساليب الإثبات القانوني في مختلف أنحاء العالم، حيث أدت الثورة الرقمية إلى تغييرات جذرية في طريقة إجراء المعاملات القانونية. فقد أصبح من الممكن استخدام الأدلة الرقمية مثل الكتابة الإلكترونية، البريد الإلكتروني، التوقيعات الرقمية، والوثائق الإلكترونية كوسيلة قانونية معترف بها في معظم الأنظمة القضائية. على المستوى الدولي، تبنت العديد من البلدان تشريعات تسهل قبول هذه الأدلة في المحاكم، مما يعكس التحول الكبير في مفهوم الإثبات القانوني في العصر الرقمي.

أما في الجزائر، فقد شهدت التشريعات تطورًا مشابهًا، حيث قام المشرع بتعديل القانون المدني في 2005 ليعترف بالكتابة الإلكترونية كوسيلة إثبات قانونية. كما تم **إصدار** قانون التوقيع والتصديق الإلكتروني رقم 15-04 في 2015، مما ساهم في تعزيز مصداقية الأدلة الإلكترونية في المعاملات المدنية. في هذا الإطار، سنتناول في هذه الدراسة كيفية تأثير تكنولوجيا الإعلام والاتصال على الإثبات القانوني المدني، سواء على المستوى الدولي أو في النظام القانوني الجزائري، مع التركيز على التحديات التي تطرحها هذه التكنولوجيات في قبول الأدلة الرقمية أمام القضاء.

من خلال هذه الدراسة، سنتعرض لحجية أدلة الإثبات الإلكتروني في المجال المدني، حيث نركز على الكتابة الإلكترونية والتوقيع الإلكتروني كأدوات قانونية معترف بها دوليا وفي الجزائر،

مع تسليط الضوء على التحديات القانونية والتقنية المرتبطة بها، وكيفية تعامل القضاء مع هذه الأدلة في إطار النظام القانوني الجزائري.

الفرع الأول: الكتابة الإلكترونية كوسيلة إثبات في المعاملات الرقمية

مع التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصال، أصبح من الضروري تحديث أساليب الإثبات القانونية لمواكبة التطور الرقمي. بعد أن كانت الوثائق الورقية هي القاعدة التقليدية للإثبات، أدى ظهور المعاملات الإلكترونية إلى الحاجة لإعادة النظر في قانون الإثبات، خصوصًا مع الاعتماد المتزايد على الوسائل الرقمية. وبذلك، تم اعتماد الكتابة الإلكترونية كأداة قانونية معترف بها، ما يعكس تحولًا مهمًا في كيفية التعامل مع الأدلة القانونية . ومع هذا التحول الرقمي، أصبح من الضروري أن تواكب التشريعات القانونية مثل قانون الإثبات في الجزائر هذا التغيير لضمان قبول الكتابة الإلكترونية وتحديد مدى حجيتها القانونية في الإثبات أمام القضاء.

أولا: مفهوم الكتابة الإلكترونية

أدى التطور التكنولوجي في وسائل الإعلام والاتصال إلى ظهور ما يُعرف بالكتابة الإلكترونية كأداة لإثبات المعاملات القانونية. وهذه الكتابة لا تقتصر على الوثائق التقليدية بل تشمل أي نوع من المعلومات المدونة على دعامات إلكترونية، بحيث يمكن فهم محتواها عند الحاجة. وقد تعرض العديد من الفقهاء والمشرعين لتحديد مفهوم الكتابة الالكترونية، مع اختلافها في التسمية التي اعطوها اليها [58]، وقد عرفها البعض بأنها "مجموعة من الحروف، الأرقام، الرموز أو الإشارات المدونة على دعامة إلكترونية أو رقمية أو ضوئية، بحيث تكون قابلة للإدراك"[59]. وقد تناول كل من قانوني الأونسيترال النموذجيين بشأن التجارة الالكترونية والتوقيعات الالكترونية، تحديد مفهوم رسالة البيانات ونصا على أنّها :" المعلومات التي يتم إنشاؤها أو إرسالها أو إنشاؤها أو استلامها أو تخزينها بوسائل الكترونية أو ضوئية أو بوسائل مشابهة ، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الالكترونية ،أو البريد الالكتروني ،أو البرق ،أو التلكس أو النسخ البرقي[60]".

وقد تبنى المشرع الجزائري في تعديلاته لقانون الإثبات المدني سنة 2005 تعريفًا غير مباشر للكتابة الإلكترونية، حيث نص في المادة (323 مكرر) من القانون المدني على أن " ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أية علامات أو رموز ذات معنى مفهوم

---

[58] - فمنهم من سموها ب مصطلح "رسالة البيانات" و"السجل الالكتروني" مثل قانون الأونسترال والتشريع الاردني، وهناك من سماها ب الوثيقة الالكترونية الذي استخدمه التشريع التونسي ومنها من سماها بمصطلح "المحرر الالكتروني" مثل التشريع المصري. في حين استخدم المشرع الجزائري مصطلح "الكتابة المتخذة شكلاً الكترونيا أو الكتابة على دعامة الكترونية.

[59] - جمال عبد الرحمن محمد علي، الحجية القانونية للمستندات الإلكترونية، بدون دار للنشر، 2004، ص09.

[60] - المادة (01) من قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية والمعتمد رسميا من قبل اللجنة العامة للأمم المتحدة بموجب القرار51 / 162 الصادر بتاريخ 16 ديسمبر 1996، والمادة (02/ج) من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية الصادر عن الجمعية العامة للأمم المتحدة بموجب القرار رقم 80/56 المؤرخ بتاريخ 12 ديسمبر 2001.

مهما كانت الوسيلة التي تتضمنها، وكذا طرق إرسالها". هذا التعريف يواكب التطور التكنولوجي ويشمل جميع أنواع الكتابات، سواء كانت على وسائط ورقية أو إلكترونية[61].

يتضح من نص المادة الواردة في القانون المدني الجزائري أن المشرع لم يضع تعريفًا محددًا للكتابة الإلكترونية، بل وسّع مفهوم الكتابة ليشمل جميع أشكالها، سواء كانت ورقية أو إلكترونية أو مستقبلاً أي وسيلة أخرى يفرزها التطور التكنولوجي، وذلك من خلال تبنيه لمبدأ الحياد التقني. ويعني هذا المبدأ عدم التمييز بين مختلف الدعامات المستخدمة في توثيق الكتابة، ما دامت تتيح التعبير عن معانٍ واضحة ومفهومة للأطراف المعنية، وللقضاء في حالة نشوء نزاع حولها. وبذلك يمكن اعتبار الكتابة الإلكترونية أي نص يتضمن حروفًا، أرقامًا، أو رموزًا مدونة على وسيلة إلكترونية، شريطة أن تكون قابلة للإدراك والفهم لضمان قيمتها القانونية في الإثبات.

ثانيا: أنواع الكتابة الالكترونية

1- الكتابة الالكترونية الرسمية:

تُعرَّف الكتابة الرسمية في الإثبات القانوني على أنها الوثيقة التي يحررها موظف عام أو شخص مكلف بخدمة عامة، وفقًا للأشكال القانونية المحددة، لإثبات ما تلقاه من ذوي الشأن. ومع الاعتراف بالإثبات الإلكتروني، أُثير تساؤل حول إمكانية إنشاء كتابة رسمية إلكترونية تمنح ذات الحجية القانونية للكتابة الورقية. وكان المشرع الفرنسي من أوائل من أقر بذلك عبر المادة 1317-2 من القانون المدني، التي سمحت بإنشاء محرر رسمي إلكتروني شريطة الامتثال للضوابط التي حددها مرسوم صادر عن مجلس الدولة، وهو ما تم تكريسه في المرسومين رقم 973-2005 و972-2005 الصادرين في 10 أغسطس 2005، اللذين وضعا معايير لإنشاء وحفظ الكتابة الرسمية الإلكترونية بالنسبة للموثقين والمحضرين القضائيين[62]..

تنقسم الكتابة الرسمية الإلكترونية في التشريع الفرنسي إلى نوعين: الأول هو الكتابة الرسمية المحررة على دعامة إلكترونية، وهي مماثلة للكتابة التقليدية من حيث الشروط والإجراءات لكنها تُنشأ رقمياً، دون أن يعني ذلك إمكانية إتمامها عن بعد. أما النوع الثاني، فهو الكتابة الرسمية الإلكترونية بالمعنى الدقيق، حيث يتم تحريرها عبر وسائل إلكترونية دون حضور مادي للأطراف، مما استدعى وضع ضوابط لضمان تحقيق الرسمية، كما ورد في المادة 1317-2 من القانون المدني والمادة 20 من المرسوم 71-941 المعدل بالمرسوم 973-2005، والتي اشترطت حضور كل طرف أمام موظف عام ضمن دائرة إقامته لضمان صحة الإجراءات وحجية المحرر

ويتطلب إنشاء الكتابة الرسمية الإلكترونية بمشاركة أكثر من موظف عام نظامًا تقنيًا متقدّمًا، نصت عليه المادتان 16 من المرسوم 973-2005 و26 من المرسوم 972-2005، حيث يُلزم

---

[61] - محمد احمد كاسب خليفة، الاثبات والالتزامات في العقود الالكترونية دار الفكر الجامعي، االاسكندرية، ص 275.

[62]- عابد فايد عبد الفتاح فايد، الكتابة الالكترونية في القانون المدني" الفكرة والوظائف"، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق ، بجامعة حلوان، مصر، 2008، ص 191 وما بعدها.

الموثقون والمحضرون القضائيون باستخدام نظام معتمد لضمان سلامة وسرية الوثائق. ورغم تطابق الشروط القانونية بين الكتابة الرسمية الورقية والإلكترونية، فإن الطبيعة الرقمية فرضت متطلبات خاصة، أبرزها اشتراط التوقيع الإلكتروني المؤمن للموثق والمحضر القضائي وفقًا للمرسوم 272-2001 لضمان الحماية من التعديل، بينما لم يُلزم المشرّع ذوي الشأن باستخدام توقيعات إلكترونية مؤمنة، مكتفيًا بوسيلة تعرض توقيعاتهم اليدوية بصيغة مرئية على الشاشة.

ولم ينص المشرع الجزائري صراحة على إمكانية إنشاء كتابة رسمية إلكترونية كما فعل المشرع الفرنسي. ويعود ذلك إلى غياب نصوص قانونية تجيز التوثيق الإلكتروني[63]، إضافةً إلى تأكيد القضاء الجزائري على الحضور المادي للموثق وأطراف العقد. ويتطلب الاعتراف بالكتابة الرسمية الإلكترونية نصوصًا واضحة تنظم عمل الموثق الإلكتروني، وتوفير شبكة داخلية تربط مكاتب التوثيق لضمان سلامة تبادل الوثائق. وقد نجح المشرع الفرنسي في وضع إطار قانوني محكم يحقق مساواة فعلية بين الكتابة الرسمية الإلكترونية والورقية، وهو نهج يُستحسن أن يتبناه المشرع الجزائري لضمان حجية هذه الكتابة في الإثبات.

2- الكتابة الالكترونية العرفية : وهي نوعان:

2-1- **الكتابة العرفية الإلكترونية المعدة للإثبات:** هي تلك التي تتم عبر وسيلة إلكترونية، وتستوفي الشروط الأساسية التي تضمن صحة الإثبات في الكتابة العرفية الورقية، مثل تحديد الواقعة وتوقيع الأطراف المعنيين[64]. الفرق الرئيسي يكمن في أن هذه الكتابة تأخذ شكلاً إلكترونياً يتناسب مع الطبيعة الرقمية للوسيلة المستخدمة، مثل استخدام التوقيع الإلكتروني بدلاً من التوقيع اليدوي. وتشمل القواعد العامة للإثبات في الكتابة العرفية الإلكترونية ضرورة ضمان صحة التوقيع والتأكد من هوية الأطراف المتعاقدة.

فيما يتعلق بالكتابة العرفية الإلكترونية في التشريع الفرنسي، أضاف المشرع شرطين أساسيين لصحتها بجانب الكتابة والتوقيع. أولاً، اشترط تعدد النسخ الأصلية للكتابة العرفية بنص المادة 1325 من القانون المدني الفرنسي، بحيث يتم إعداد نسخة لكل طرف من أطراف العقد. وإذا تم تجاهل هذا الشرط، فإن الكتابة تكون باطلة، مع إمكانية اعتبارها مبدأ ثبوت بالكتابة. ثانياً، تتيح المادة 1325 المعدلة بموجب المرسوم رقم 274-2005 تطبيق هذا الشرط على الكتابة العرفية الإلكترونية إذا تم إعدادها وفقاً للمعايير التقنية التي تتيح لكل طرف الحصول على نسخة من الكتابة. بالإضافة إلى ذلك، اشترط المشرع الفرنسي بموجب المادة 1326 من القانون المدني ضرورة أن يتضمن السند الإلكتروني إثبات التصرفات القانونية الملزمة لجانب واحد، مثل دفع المبالغ المالية أو تسليم مال مثلي، مع تضمين السند توقيع الملتزم وتحديد المبلغ أو الكمية بالحروف والأرقام.

فيما يخص موقف المشرع الجزائري، فقد اعترف بالكتابة الإلكترونية كأداة قانونية معترف بها للإثبات من خلال تعديلاته في القانون المدني. وقد نصت المادة 323 مكرر من القانون المدني الجزائري على جواز الاعتداد بالكتابة والتوقيع الإلكتروني في الإثبات، بشرط أن تكون الكتابة

---

[63] - لم يتعرض القانون رقم 06-02 المتعلق بتنظيم مهنة الموثق للنظام القانوني للكتابة الرسمية في الشكل الالكتروني ، الصادر بتاريخ 20 فيفري 2006، الجريدة الرسمية عدد 14 مؤرخة في 08 مارس 2006، الصفحة 15.

[64] - مساعد صالح نزال الشمري، دور السندات العادية في الاثبات" دراسة مقارنة بين القانونين الأردني والكويتي"، مذكرة ماجستير بجامعة الشرق الأوسط، 2012، ص 41 وما بعدها.

معدة ومحفوظة في ظروف تضمن سلامتها، مع التأكد من هوية الشخص الذي أصدرها. كما نصت المادة (327): " يعتبر العقد العرفي صادرا ممن كتبه أو وقعه أو وضع عليه بصمة إصبعه ما لم ينكر صراحة ما هو منسوب إليه من خط وإمضاء... ويعتد بالتوقيع الالكتروني وفق الشروط المذكورة في المادة 323 مكرر1". ومنه المشرع الجزائري فان لم يشترط تحديد تاريخ ووقت إنشاء الكتابة الإلكترونية كما فعلت بعض التشريعات الأخرى، لكنه أكد على أهمية حفظ الكتابة في ظروف تضمن سلامتها، مما يتطلب تطوير قواعد قانونية تتناسب مع الطبيعة التقنية لهذه الكتابة.

2-**2- الكتابة العرفية غير المعدة للإثبات:** هي تلك التي تُعد عبر وسائل إلكترونية أو تقليدية لكنها لا تستوفي الشروط القانونية التي تجعلها قابلة للاعتراف بها كدليل في النزاعات القانونية. وتشمل هذه الكتابات رسائل البريد الإلكتروني، رسائل الهاتف المحمول، الفاكس، التلكس، وكذلك الدفاتر التجارية والأوراق المنزلية التي لا تحمل توقيع الأطراف المعنية. ورغم أنها قد لا تكون موقعة من ذوي الشأن، فإن القانون المقارن يعترف ببعض حجيتها في الإثبات بناءً على ما تحتويه من عناصر قانونية قد تدعم موقف الطرف المدعي.[65].

مع التطور التقني، أصبح لهذه الكتابات غير المعدة للإثبات طابع لامادي، مما يساهم في تحديات جديدة أمام القوانين المتعلقة بالإثبات. فعلى الرغم من أن هذه الكتابات لم تُعد بغرض استخدامها كدليل قانوني، فإن التقدم في وسائل الاتصال جعلها تدخل في إطار الحاجات القانونية، ما يستدعي تطوير قواعد قانونية تواكب التغيرات التكنولوجية وتحدد في أي الحالات يمكن استخدامها كوسيلة لإثبات الحقوق.

ثالثا: الشروط الأساسية لقبول الكتابة الإلكترونية كدليل قانوني

تشترط التشريعات القانونية، بما في ذلك المشرع الجزائري، عدة معايير ضرورية لضمان قبول الكتابة الإلكترونية كدليل قانوني معترف به في الإثبات، وذلك لضمان تماثلها مع الكتابة الورقية التقليدية في حجيتها. من أبرز هذه الشروط: القدرة على قراءة النص بوضوح، ضمان الثبات وعدم التعديل، وتحديد هوية الشخص الذي أصدر الكتابة الإلكترونية.

بداية يشترط في الكتابة الإلكترونية أن تكون قابلة للقراءة أو الفهم بسهولة، بمعنى أن النصوص والرموز التي تحتوي عليها يجب أن تكون واضحة ومفهومة. المشرع الجزائري أكد هذا الشرط في المادة 323 مكرر من القانون المدني، حيث نص على ضرورة أن يكون النص المدون عبر وسيلة إلكترونية قابلًا للفهم بأي وسيلة كانت، بما في ذلك الرموز أو الأرقام، طالما أن الوسيلة المستخدمة لنقلها تضمن وضوح المحتوى.

كما يشترط كذلك أن يتم حفظ الكتابة الإلكترونية في وسيط يسمح بالحفاظ على محتوياتها بشكل ثابت، بحيث لا يمكن تعديلها أو تلاعبها[66]. هذا الشرط يتضمن ضمان سلامة الوثيقة الإلكترونية بحيث تظل كما هي عند إصدارها دون أي تغيير غير مصرح به، وهو ما أكده المشرع الجزائري في المادة 323 مكرر 01، حيث نص على ضرورة التأكد من حفظ الكتابة في ظروف

---

[65] - ينظر في ذلك نصوص المواد (329) الى (323) من القانون المدني الجزائري

[66] - الصالحين محمد العيش، دور الدليل الالكتروني في اثبات المعاملات المصرفية" عرض وتقييم لموقف القانون الليبي"، مؤتمر المعاملات الإلكترونية (التجارة الالكترونية – الحكومة الإلكترونية)، المؤتمر الدولي السابع عشر بجامعة الامارات العربية المتحدة ، كلية القانون ، أبو ظبي، 19 و20 ماي 2009، ص 679..

تضمن سلامتها. يشير هذا إلى ضرورة استخدام وسائل تخزين آمنة ومؤمنة تضمن استمرارية الوثيقة وموثوقيتها لفترات طويلة.

أخيرًا، من الضروري أن يتم تحديد هوية الشخص الذي أصدر الكتابة الإلكترونية، وذلك لضمان أن تكون هذه الكتابة موثوقة وقابلة للاعتراف بها في المحكمة. وقد تم التأكيد على هذا الشرط في نصوص متعددة، مثل قانون الأونسترال للتجارة الإلكترونية، وكذلك في المادة 323 مكرر 01 من القانون المدني الجزائري التي تشترط أن يكون بالإمكان تحديد هوية الشخص الذي أصدر الكتابة الإلكترونية لضمان حجيتها القانونية.

رابعا: المساواة القانونية بين الكتابة الإلكترونية والورقية في الإثبات

تعتبر الكتابة الإلكترونية أداة قانونية هامة في عصر التكنولوجيا الرقمية، وقد تبنت العديد من التشريعات الحديثة مبدأ المساواة في الحجية القانونية بين الكتابة الإلكترونية والكتابة الورقية[67]. هذا المبدأ يُعرف في الفقه القانوني بـ "التعادل الوظيفي" بين النوعين، حيث يتم التعامل مع الكتابة الإلكترونية بنفس القدر من الجدية والاعتبار الذي يُعطى للكتابة الورقية في الإثبات.

لقد تبنت التشريعات المقارنة، بما فيها التشريع الجزائري، هذا المبدأ في سياق المعاملات الإلكترونية. على سبيل المثال، نصت المادة 323 مكرر من القانون المدني الجزائري على أن الكتابة الإلكترونية تُعتبر حجتها القانونية معادلة لتلك المقررة للكتابة الورقية، شريطة أن تتوافر فيها بعض الشروط التقنية مثل إمكانية تحديد هوية الشخص الذي أصدرها، وضمان حفظها في ظروف تضمن سلامتها. كما أقر المشرع الفرنسي هذا المبدأ في المادة 1316-1 من القانون المدني الفرنسي، حيث يتم التعاطي مع الكتابة الإلكترونية بنفس الطريقة التي تُتعامل بها مع الكتابة الورقية.

ويشمل ذلك جميع أنواع الكتابات الإلكترونية، بما في ذلك المحررات الرسمية والعرفية، حيث يتم منح الكتابة الإلكترونية ذات الحجية القانونية التي تتمتع بها الكتابة الورقية التقليدية. إلا أن هذا التعادل في الحجية قد يتطلب تطبيق قواعد خاصة تتعلق بالإثبات الإلكتروني، نظرًا للخصوصيات التقنية لهذه الكتابة. ومن هنا تنشأ الحاجة إلى تنظيم قانوني خاص للتأكد من قبول الكتابة الإلكترونية كدليل قانوني معتمد أمام القضاء.

الفرع الثاني: التوقيع الإلكتروني كوسيلة إثبات في المعاملات الرقمية

في ظل الثورة الرقمية التي تشهدها تكنولوجيا الإعلام والاتصال، أصبح التوقيع الإلكتروني أداة حيوية لضمان مصداقية المعاملات الرقمية وحمايتها من التلاعب. تتيح هذه التكنولوجيا الجديدة للأفراد والمؤسسات إجراء المعاملات الإلكترونية بشكل سريع وآمن، سواء كان ذلك في إبرام العقود أو تبادل الوثائق الحساسة. من خلال استخدام تقنيات مثل التشفير والأدوات الرقمية، يعزز التوقيع الإلكتروني من مستوى الثقة بين الأطراف المتعاملة، مما يضمن سلامة البيانات ويجعلها قابلة للإثبات قانونياً. وبالتالي، فإن التوقيع الإلكتروني لا يمثل مجرد وسيلة لتوثيق الهوية، بل هو ركيزة أساسية تضمن شفافية وموثوقية المعاملات في عصر تكنولوجيا الإعلام والاتصال.

---

[67] - أيمن عبد الله فكري الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصد، الرياض، الطبعة الأولى، 2014، ص 483. محمد احمد كاسب خليفة، المرجع السابق، ص 301.

أولا تعريف التوقيع الالكتروني

تناول الفقه تعريف التوقيع الإلكتروني من زوايا متعددة[68]، حيث تم التركيز على الجوانب التقنية والوظيفية له. فبعض التعريفات ربطت التوقيع بالرموز، الأرقام أو الحروف المشفرة، بينما رأى آخرون أنه وسيلة تتيح تحديد هوية الشخص الموقع وتوثيق قبوله للمحتوى. أفضل التعريفات هي تلك التي تدمج بين الجانبين، التقني والوظيفي، حيث يُعرف التوقيع الإلكتروني بأنه: "مجموعة من الإجراءات التقنية التي تشمل رموزًا أو أرقامًا أو حروفًا أو إشارات إلكترونية، ترتبط بشكل موثوق بالبيانات الإلكترونية وتسمح بتحديد هوية الموقع، فضلًا عن إظهار قبوله للمحتوى المرتبط بالتوقيع، بما يضمن سلامة الوثيقة".

وعرّفه المشرع الجزائري في المادة 2 من القانون رقم 15-04 المؤرخ في 1 فيفري 2015 والمتعلق بالتوقيع والتصديق الإلكترونيين، حيث نص على أنه: "بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقياً ببيانات إلكترونية أخرى تستعمل كوسيلة للتوثيق". يُظهر التعريف أن المشرع الجزائري تبنى مفهوماً واسعاً للتوقيع الإلكتروني يشمل مختلف التقنيات المستخدمة لتحقيق المصادقة القانونية. وهو بيانات إلكترونية رقمية :أي انه ليس عنصراً مادياً، كما انه لا يكون مستقلاً، بل مرتبطاً منطقياً بمستند إلكتروني معين. ووظيفتة التوثيق :أي إثبات صحة الوثيقة وهوية الموقع.

ثانيا: أنواع التوقيع الالكتروني:

لقد أدى تطور التكنولوجيا في مجال نقل وتبادل المعلومات إلى ظهور أشكال جديدة من التوقيع الإلكتروني، والتي تزداد تطورًا وتتكيف مع التطورات المستقبلية في تكنولوجيا المعلومات والاتصالات. وفي هذا السياق، عمل الفقهاء على تصنيف هذه الأشكال استنادًا إلى مستوى الأمان والموثوقية الذي توفره. ومن خلال هذه التصنيفات، يظهر التوقيع الإلكتروني في ثلاثة مستويات رئيسية :**التوقيع الإلكتروني البسيط، التوقيع الإلكتروني المؤمن، والتوقيع الإلكتروني الموصوف.**

1. **التوقيع الإلكتروني البسيط** :هو الأكثر بساطة في وسائل تنفيذه، ويشمل التوقيع باستخدام البريد الإلكتروني، أو الضغط على زر الموافقة في التطبيقات، أو التوقيع باستخدام صورة رقمية عبر الماسح الضوئي. هذا النوع من التوقيع لا يتطلب شهادة تصديق أو تقنيات معقدة، ولكن يجب أن يتماشى مع شروط الكتابة الإلكترونية من حيث التأكد من هوية الشخص وضمان سلامة البيانات الموقعة. على الرغم من أنه يُعتبر أقل أمانًا، إلا أنه مقبول قانونيًا إذا كان مرفقًا بأدلة تؤكد هوية الموقع. مثال على ذلك هو توقيع عقد عبر الإنترنت باستخدام البريد الإلكتروني أو تأكيد العمليات عبر التطبيقات باستخدام كلمة مرور.
2. **التوقيع الإلكتروني المؤمن** :يعتمد هذا النوع على تقنيات التشفير الرقمي ويتطلب شهادة تصديق إلكترونية معترف بها. يضمن التوقيع المؤمن مستوى عالٍ من الأمان من خلال ربطه بالموقع بشكل حصري باستخدام وسائل يمكن للموقع التحكم فيها. كما يتم ضمان صحة البيانات الموقعة وإمكانية الكشف عن أي تعديل لاحق. يُستخدم هذا النوع في المعاملات التي

[68] - خالد ممدوح إبراهيم الاثبات الالكتروني في المواد الجنائية والمدنية دار الفكر الجامعي الاسكندرية ص 233.

تتطلب درجة أمان أعلى، مثل المعاملات المالية والعقود التجارية الكبرى. مثال على ذلك هو توقيع عقد عبر الأنظمة المصرفية التي تستخدم شهادات تصديق رقمية.

3. **التوقيع الإلكتروني الموصوف** :يعد هذا النوع الأكثر أمانًا ويُستخدم في المعاملات التي تتطلب توثيقًا قويًا، مثل المعاملات الحكومية أو العقود الرسمية. يعتمد التوقيع الموصوف على شهادة تصديق إلكترونية موصوفة ويُنشأ باستخدام آلية مؤمنة تضمن إمكانية التحقق من هوية الموقع وصحة البيانات الموقعة. يعتبر هذا النوع من التوقيع هو الأقوى قانونيًا ويُستخدم في المعاملات الحساسة. مثال على ذلك هو توقيع العقود الحكومية أو الاتفاقيات الدولية عبر منصات معتمدة.

موقف المشرع الجزائري من هذه الأنواع يظهر من خلال قانون التوقيع والتصديق الإلكتروني رقم 15-04 الصادر في 1 فيفري 2015، والمرسوم التنفيذي رقم 07-162 الصادر في 30 ماي 2007، حيث تبنى المشرع الجزائري التصنيف الثلاثي لمستويات التوقيع الإلكتروني المتفق عليها دوليًا، وهو التصنيف الذي يواكب التنظيم الأوروبي رقم 910-2014.

- **التوقيع الإلكتروني البسيط** :كما تم تحديده في المادة 03 مكرر من المرسوم التنفيذي رقم 07-162، يتمثل في "معطى ينجم عن استخدام أسلوب عمل يستجيب للشروط المحددة في المواد 323 مكرر و323 مكرر 1 من الأمر رقم 75-58"، ويُعتبر هذا التوقيع مقبولًا إذا كان مرفقًا بأدلة تؤكد هوية الشخص الموقّع وسلامة البيانات.
- **التوقيع الإلكتروني المؤمن** :وفقًا للمادة 03 مكرر من المرسوم التنفيذي، يتم تعريفه على أنه توقيع إلكتروني يفي بالمتطلبات التي تضمن ارتباطه بالموقع بشكل حصري، واستخدام وسائل يمكن للموقع التحكم فيها، وتوفير الكشف عن أي تعديل لاحق للبيانات الموقعة.
- **التوقيع الإلكتروني الموصوف** :كما جاء في المادة 07 من قانون 15-04، يعتمد على شهادة تصديق إلكترونية موصوفة ويجب أن يُنشأ باستخدام آلية مؤمنة خاصة بإنشائه. هذا النوع من التوقيع يضمن أقصى درجة من الأمان ويُستخدم في المعاملات الرسمية والقانونية التي تتطلب توثيقًا عاليًا[69].

بالمجمل، يسعى المشرع الجزائري بشكل عام إلى تبني الأنماط العالمية المعترف بها في مجال التوقيع الإلكتروني، مع ضرورة توفير إطار قانوني يتناسب مع كل نوع من أنواع التوقيع، حسب مستوى الأمان والموثوقية المطلوب. ورغم وضوح التصنيف الثلاثي الذي تم اعتماده، إلا أن بعض المصطلحات القانونية في القانون الجزائري قد تحتاج إلى مزيد من التوضيح والدقة، لتسهيل الفهم وضمان تطبيق أكثر فعالية.

ثالثا: الشروط الأساسية للاعتداد بالتوقيع الإلكتروني:

[69] - المادة (07) من القانون رقم 15-04 للتوقيع والتصديق الالكتروني الجزائري التي نصت على أنّ:" التوقيع الالكتروني الموصوف هو الذي تتوافر فيه المتطلبات التالية: 1- أن ينشأ على أساس شهادة تصديق إلكترونية موصوفة. 2- أن يرتبط بالموقع دون سواه، 3- أن يمكن من تحديد هوية الموقع، 4- أن يكون مصمماً بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الالكتروني، 5- أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع، 6- أن يكون مرتبطاً بالبيانات الخاصة به بحيث يمكن الكشف عن التغييرات اللاحقة بهذه البيانات"

تتفق جميع التشريعات الدولية والإقليمية والوطنية المتعلقة بالتوقيع الإلكتروني على ضرورة توافر شروط قانونية محددة للاعتداد بالتوقيع الإلكتروني في الإثبات[70]. وقد تناول المشرع الجزائري كذلك هذه الشروط في قانون التوقيع والتصديق الإلكترونيين رقم 15-04 الصادر في 1 فبراير 2015، وكذلك في المرسوم التنفيذي رقم 07-162 المتعلق بنظام الاستغلال المطبق على أنواع الشبكات المختلفة وخدمات المواصلات الصادرة في 30 مايو 2007. وهذه الشروط تتشابه في مضمونها بين التشريعات المختلفة، مع وجود اختلافات بسيطة في صياغتها. وهي تتمثل في التالي:

1.شرط تحديد التوقيع الإلكتروني لهوية الموقع وارتباطه به بشكل حصري

يشترط المشرع الجزائري أن يكون التوقيع الإلكتروني قادرًا على تحديد هوية الشخص الموقع عليه بشكل دقيق وفريد، بحيث يرتبط هذا التوقيع بالشخص الموقع فقط دون أي تدخل من آخرين. ويعد هذا الشرط أساسيًا لضمان أن التوقيع يعكس إرادة الموقع بدقة، مما يسهم في حماية العمليات القانونية التي يتم فيها استخدام التوقيع الإلكتروني.

ويمكن إثبات شرط تحديد التوقيع الإلكتروني لهوية الموقع وارتباطه به لوحده دون غيره من خلال عدة آليات قانونية وتقنية تضمن مصداقيته كتقارير الخبرة التي يلجأ إليها القاضي[71] ، كما تتيح شهادات التصديق الإلكتروني التي تصدرها جهات معتمدة توثيق هوية الموقع وربط التوقيع به حصريًا. كما تساعد تقنيات التشفير في ضمان عدم إمكانية التلاعب بالتوقيع، حيث يؤدي أي تعديل في البيانات إلى إبطال صحته. بالإضافة إلى ذلك، يمكن استخدام التحقق البيومتري مثل بصمات الأصابع أو التعرف على الوجه لربط التوقيع بالشخص ذاته. وتعزز أنظمة التحقق متعدد العوامل (MFA) موثوقية التوقيع من خلال إضافة طبقات أمان إضافية، مثل إرسال رمز تحقق إلى الهاتف المحمول. وأخيرًا، تلعب الجهات الموثوقة مثل شركات التوثيق الإلكتروني والمؤسسات المالية دورًا في تأكيد صحة التوقيع وهوية الموقع، مما يوفر ضمانات قانونية إضافية..

2.شرط سيطرة الموقع الحصرية على وسائل إنشاء التوقيع الإلكتروني

يتطلب القانون الجزائري أن يكون للموقع سيطرة كاملة وحصرية على الأدوات والوسائل التي يستخدمها لإنشاء التوقيع الإلكتروني. وهذا يعني أن الشخص الذي يقوم بالتوقيع هو الوحيد

---

[70] - ينظر في ذلك إلى المادة (3/6/ ب) من قانون الاونسترال بشأن التوقيعات الالكترونية لعام 2001 الفقرات 11 و12 من المادة (03) والمادة (26) والملحقين I و II من التنظيم الاوروبي رقم 910-2014 الصادر بتاريخ 23 جويلية 2014، وكذلك المادتين (01 و02) من المرسوم الفرنسي رقم 2001-272 الصادر بتاريخ 30 مارس 2001

[71]- تنص المادة (125) من قانون الإجراءات المدنية و الإدارية الجزائري على أن:" تهدف الخبرة إلى توضيح واقعة مادية تقنية أو علمية محضة للقاضي"، وأخضع المشرع الجزائري الخبرة للسلطة التقديرية للقاضي الذي يقدر مدى ضرورة الاستعانة بها ويملك السلطة المطلقة في ندب الخبير من تلقاء نفسه أو عدم ندبه متى رأى أسباباً سائغة لذلك، حيث نصت المادة (126) من ذات القانون على أنه:" يجوز للقاضي من تلقاء نفسه أو بطلب من أحد الخصوم تعيين خبير أو عدة خبراء من نفس التخصص أو من تخصصات مختلفة". ينظر قانون الاجراءات المدنية والإدارية الجزائري رقم 08-09 المؤرخ في 25 فيفري 2008 الصادر بالجريدة الرسمية الصادرة بتاريخ 23 افريل 2008 عدد 21، ص 13.

الذي يمتلك السيطرة على الوسيلة المستخدمة، مثل جهاز الكمبيوتر أو البرنامج الإلكتروني، مما يقلل من المخاطر المتعلقة بالاختراقات أو التلاعب في عملية التوقيع.

لذلك، نجد أن بعض التشريعات المقارنة قد حرصت على توضيح كيفية تحقق شرط سيطرة الموقع الحصرية على وسائل إنشاء التوقيع الإلكتروني، ومن بينها التشريع المصري، الذي نصت لائحته التنفيذية لقانون التوقيع الإلكتروني في مادته العاشرة على أن هذه السيطرة تتحقق من الناحية الفنية والتقنية عندما يكون الموقع هو الوحيد الذي يحوز الوسيط الإلكتروني المستخدم في تثبيت التوقيع. ويتم ذلك عبر امتلاكه لأداة حفظ المفتاح الشفري الخاص[72]، والتي قد تشمل البطاقة الذكية المؤمنة والكود السري المرتبط بها، مما يضمن عدم إمكانية استخدامها من قبل أي شخص آخر.

3.شرط الكشف عن أي تعديل أو تغيير لاحق للبيانات المدرج عليها التوقيع الإلكتروني

أحد الشروط الأساسية التي يفرضها المشرع الجزائري هو أن يكون التوقيع الإلكتروني قادرًا على الكشف عن أي تعديل أو تغيير لاحق قد يُجرى على البيانات التي تم توقيعها. هذا يعني أن التوقيع يجب أن يكون حساسًا لأي تغيير يُحدث بعد عملية التوقيع، وبالتالي يمكن اكتشاف التلاعب بالبيانات بسهولة، مما يساهم في الحفاظ على صحة الوثائق الإلكترونية الموقعة.

4.شرط اعتماد التوقيع الإلكتروني على شهادة تصديق إلكتروني موصوفة

يشترط القانون الجزائري أن يتم التوقيع الإلكتروني باستخدام شهادة تصديق إلكتروني موصوفة، وهي شهادة تُمنح من قبل جهة معترف بها قانونًا. هذه الشهادة تضمن صحة التوقيع الإلكتروني وتساعد في تعزيز موثوقية الوثائق الإلكترونية الموقعة، مما يمنح الأطراف المتعاملة مع هذه الوثائق ضمانًا قانونيًا في حال حدوث أي نزاع.

5.شرط إنشاء التوقيع الإلكتروني بواسطة آلية موصوفة

وفقًا للتشريع الجزائري، يجب أن يتم إنشاء التوقيع الإلكتروني باستخدام آلية محددة وموصوفة وفق معايير أمان دقيقة. هذه الآلية تضمن أن التوقيع يتم بطريقة محمية ومؤمنة ضد أي محاولات للتلاعب أو التزوير، مما يعزز من سلامة الوثائق الموقعة إلكترونيًا ويحافظ على مصداقيتها القانونية[73].

---

[72] - يعرف المشرع الجزائري في المادة (8/2) من قانون التوقيع والتصديق الالكترونيين رقم 15-04 مفتاح التشفير الخاص بأنّه:" عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني ويرتبط هذا المفتاح بمفتاح تشفير عمومي"، مفتاح التشفير العمومي الذي هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور لتمكينهم من التحقق من شخصية الموقع والتأكد من صحة وسلامة البيانات الأصلية المدرج عليها التوقيع الالكتروني وتوضع على شهادة التصديق الالكتروني" يراجع المادة (9/2) من قانون التوقيع والتصديق الالكترونيين رقم 15-04 الجزائري

[73] - لمادة 15 من قانون التوقيع والتصديق الالكتروني الجزائري

تحدد التشريعات الشروط اللازمة لجعل آلية إنشاء التوقيع الإلكتروني موصوفة أو مؤمنة، وهي كالتالي: ضمان سرية البيانات المستخدمة، أن تكون البيانات فريدة وغير قابلة للتكرار، وألا يمكن الوصول إليها عن طريق الاستنتاج. كما يجب حماية التوقيع من التزوير، وضمان عدم استخدامه من قبل الغير، وكذلك منع تعديل البيانات الموقعة قبل التوقيع عليها. مع عدم إمكانية إحداث أي إتلاف أو تعديل بمضمون البيانات المراد توقيعه[74]ا. وتوافر هذه الشروط يعزز من تحديد هوية الموقع، ويجعل التوقيع مرتبطًا به حصريًا، ويسمح له بالكشف عن أي تعديل أو تغيير في البيانات الموقعة.

رابعا: حجية التوقيع الإلكتروني في الإثبات

إن التوقيع الإلكتروني، إذا استوفى الشروط القانونية المحددة له، يتمتع بحجية قانونية مشابهة لتلك التي يتمتع بها التوقيع الخطي التقليدي. وهذا ما يعرف بمبدأ "التكافؤ الوظيفي" بين التوقيع الإلكتروني الموثوق والتوقيع الخطي المكتوب. في العديد من التشريعات الوطنية والدولية، يعتبر التوقيع الإلكتروني المستوفي لهذه الشروط مساويًا للتوقيع التقليدي في قوة الإثبات.

1- إقرار التكافؤ بين التوقيع الإلكتروني المستوفي للشروط القانونية والتوقيع الخطي المكتوب

حرصت العديد من التشريعات، سواء الدولية أو الإقليمية أو الوطنية، على تأكيد مبدأ التكافؤ بين التوقيع الإلكتروني المستوفي للشروط القانونية والتوقيع الخطي المكتوب. ففي المادة 1/6 من قانون الأونسترال النموذجي بشأن التوقيعات الإلكترونية، الذي اعتمدته الجمعية العامة للأمم المتحدة في 12 ديسمبر 2001، تم التأكيد على هذا المبدأ، حيث نصت على أنه: "حينما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفيًا بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني يمكن الاعتماد عليه بالقدر المناسب للغرض الذي أنشئت أو أبلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق ذي صلة". كما نصت المادة 3 من نفس القانون على عدم تجريد أو تقييد أي طريقة من طرق إنشاء التوقيع الإلكتروني من مفعولها القانوني إذا كانت هذه الطريقة يمكن الاعتماد عليها بما يتناسب مع الغرض الذي أنشئت من أجله الرسالة الإلكترونية الممهورة بالتوقيع.

ولم يختلف المشرع الجزائري عن العديد من المشرعين الدوليين والإقليميين[75] في تكريسه نفس المبدأ المتعلق بالاعتراف بالتوقيع الإلكتروني المستوفي للشروط القانونية والاعتداد به في الإثبات. وقد جاء هذا التأكيد لأول مرة من خلال تعديل أحكام الإثبات في القانون المدني الجزائري بموجب القانون رقم 05-10 الصادر في 20 يونيو 2005، حيث أضاف المشرع فقرة ثانية للمادة 327 منه، والتي تنص على أنه: "يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر 1."

---

[74] - المادة (11) من قانون التوقيع والتصديق الالكتروني الجزائري رقم 15-04.

[75] - قانون الأونسترال النموذجي في شأن التجارة الالكترونية رقم 162/51 الذي أعدته لجنة الأمم المتحدة للقانون التجاري الدولي(CNUDCI) بتاريخ 16 جانفي 1996، المادة 7 منه. المادة (1/06) من قانون الاونسترال النموذجي بشأن التوقيعات الالكترونية الذي اعتمدته الجمعية العامة للأمم المتحدة في 12 ديسمبر 2001. المادة 2/25 من التنظيم الاوروبي رقم 910-2014 الصادر عن البرلمان الأوروبي في 23 جويلية 2014 والمتعلق بتحديد الهوية الالكترونية وخدمات التوثيق للمعاملات الالكترونية في السوق الداخلية

ورغم ذلك، فقد تم الانتقاد للمشرع الجزائري بشأن قصر تحديده لشروط موثوقية التوقيع الإلكتروني على ما يتعلق بقبول الكتابة في الشكل الإلكتروني في الإثبات، وفقًا للمادة 323 مكرر 1. ولتدارك هذا القصور، صدر القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين في 1 فبراير 2015، حيث تم توضيح الشروط القانونية والفنية المطلوبة في التوقيع الإلكتروني ليعتبر موصوفًا ويكتسب الحجية القانونية في الإثبات. وقد نصت المادة 8 من هذا القانون على أنه: "يعتبر التوقيع الإلكتروني الموصوف وحده مماثلًا للتوقيع المكتوب، سواء كان للشخص الطبيعي أو المعنوي."

2- عدم رفض التوقيع الإلكتروني غير المطابق للشروط القانونية كدليل أمام القضاء

التوقيع الإلكتروني غير المستوفي للشروط القانونية هو التوقيع الذي لا يستوفي جميع متطلبات التوقيع الإلكتروني الموصوف، ويشمل نوعين: الأول هو **التوقيع الإلكتروني البسيط،** الذي يستخدم لتحديد هوية الموقع ويظهر موافقته على المعلومات، ولكنه قد لا يضمن كفاية الموثوقية القانونية. الثاني هو **التوقيع الإلكتروني المؤمَّن،** الذي يحقق بعض متطلبات الأمان مثل تحديد هوية الموقع وضمان سرية المعطيات، ولكنه لا يصل إلى المستوى الذي يمكن مقارنته بالتوقيع الخطي المكتوب. رغم ذلك، يعتبر هذا النوع من التوقيعات مقبولاً قانونياً في العديد من التشريعات التي تمنح القضاة السلطة التقديرية في قبولها كدليل إثبات، بناءً على توفر معايير الموثوقية والأمان التي تحدد صحة التوقيع.

حيث تنص المادة 25 من التنظيم الأوروبي رقم 910-2014 على أنه لا يمكن رفض التوقيع الإلكتروني كدليل إثبات أمام القضاء لمجرد تقديمه بالشكل الإلكتروني أو عدم استيفائه لمتطلبات التوقيع الإلكتروني الموصوف، مما يعني أن التوقيع غير الموصوف لا يفقد أثره القانوني بالكامل حتى وإن لم يتم إنشاؤه عبر آلية موصوفة أو لا يعتمد على شهادة تصديق إلكتروني موصوفة. كما يقر قانون الأونسترال النموذجي لعام 2001 بأن التوقيع الإلكتروني يجب أن يفي فقط بالاشتراطات الأساسية مثل تحديد هوية الموقع والتعبير عن موافقته. وقد تبنى المشرع الجزائري نفس المبدأ في المادة 09 من القانون رقم 15-04 المتعلق بالتصديق والتوقيع الإلكترونيين، حيث نصت على أنه "بغض النظر عن أحكام المادة 08 أعلاه، لا يمكن تجريد التوقيع الإلكتروني من فعاليته القانونية أو رفضه كدليل أمام القضاء بسبب: 1- شكله الإلكتروني، 2- أنه لا يعتمد على شهادة تصديق إلكتروني موصوفة، 3- أنه لم يتم إنشاؤه بواسطة آلية مؤمنة لإنشاء التوقيع الإلكتروني."

يتساءل البعض عن القيمة القانونية للتوقيعات الإلكترونية التي لا تستوفي شروط التوقيع الإلكتروني الموصوف، حيث يرى بعض الفقه الفرنسي أنه رغم عدم تمتعها بنفس قوة التوقيع الخطي، يمكن للقضاة منحها قيمة بداية الثبوت بالكتابة إذا توفرت الشروط المطلوبة، مع إمكانية دعمها بوسائل إثبات أخرى مثل البينة والقرائ[76]ن. ويعني ذلك أنه يمكن قبول التوقيعات الإلكترونية غير المستوفية للشروط القانونية إذا كانت موثوقة بما يكفي لتحديد هوية الموقع والتعبير عن موافقته. وفي هذا السياق، قضت محكمة الاستئناف الفرنسية في 2004 بعدم قبول التوقيع باستخدام الماسح الضوئي لأنه لا يحدد هوية الموقع، وأيدت محكمة النقض الفرنسية هذا

[76] - محمد محمد السادات، حجية التوقيع الالكتروني في الاثبات، المرجع السابق، ص 321.

الحكم في 2006. كما اعتبر مجلس الدولة الفرنسي أن الرقمنة البسيطة للتوقيع لا تضمن موثوقيته بما يكفي.

تتعدد الأمثلة على التوقيعات الإلكترونية التي لا تستوفي شروط التوقيع الإلكتروني الموصوف ولكن يمكن قبولها في حالات معينة. على سبيل المثال، يمكن قبول التوقيع الممسوح ضوئيًا عبر الماسح الضوئي إذا توفرت ضمانات أخرى تؤكد صحة التوقيع، مثل شهادات إضافية أو التحقق من هوية الموقع. كما يمكن اعتبار التوقيع الذي يتم عبر البريد الإلكتروني أو منصات التواصل الاجتماعي مثل "الفيسبوك" أو "تويتر" مقبولاً، خاصة إذا كان الحساب موثقًا أو يمكن تحديد هوية الشخص المرسل بناءً على المعلومات المتاحة. هذه التوقيعات تفتقر إلى بعض متطلبات التوقيع الإلكتروني الموصوف، ولكن يمكن الاستناد إليها كدليل على الموافقة أو الإقرار بشروط معينة.

إضافة إلى ذلك، يمكن قبول التوقيع عبر بعض التطبيقات البسيطة أو منصات الدفع الإلكتروني التي تتطلب التحقق من الهوية عبر كلمات مرور أو رموز تحقق، حيث يُعتبر ذلك دليلًا على الموافقة حتى وإن كانت هذه التوقيعات لا تستوفي المعايير الأكثر تشددًا للتوقيع الإلكتروني الموصوف. في هذه الحالات، يُترك تقدير القضاة بشأن قبول هذه التوقيعات بناءً على ضمانات الأمان المتوفرة وقدرة هذه التوقيعات على تحديد هوية الموقع والتعبير عن موافقته.

المطلب الثاني: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني الجنائي

تعتبر تكنولوجيات الإعلام والاتصال (ICT) من العوامل الأساسية التي غيرت وجه العالم في القرن الواحد والعشرين، حيث أثرت بشكل عميق في مختلف جوانب الحياة الاجتماعية، الاقتصادية والقانونية. في مجال القانون الجنائي، أحدثت هذه التكنولوجيات تحولاً كبيراً في طرق جمع وتقديم الأدلة، مما فرض تحديات جديدة على المشرعين والمحاكم على حد سواء. فالأدلة الرقمية أصبحت جزءًا أساسيًا من التحقيقات الجنائية، مما يفرض على المشرع والقضاء التكيف مع هذه التطورات التكنولوجية لضمان تحقيق العدالة.

في التشريع الجزائري، كما في باقي الأنظمة القانونية، تم إدخال التكنولوجيات الحديثة في إطار الإثبات الجنائي بما يتناسب مع ما تقتضيه الوقائع الحديثة، مثل الجرائم الإلكترونية، الاحتيال الرقمي، والاختراقات الأمنية. ورغم التقدم المحرز في هذا المجال، لا تزال هناك العديد من التحديات القانونية والتقنية التي تواجه النظام القضائي، ومنها كيفية التعامل مع الأدلة الرقمية بما يتوافق مع قواعد الإثبات التقليدية وحمايتها من التلاعب أو الاستخدام غير المشروع.

الفرع الأول: الأدلة الرقمية في الإثبات الجنائي وحجيتها أمام القضاء

أولا: تعريف الدليل الالكتروني الجنائي

الدليل الرقمي في الفقه الجنائي هو المعلومات المخزنة في شكل رقمي باستخدام أجهزة الحاسوب أو الأجهزة الإلكترونية الأخرى مثل الهواتف المحمولة أو الأجهزة المتصلة بالشبكات. تختلف التعريفات المتعلقة بهذا النوع من الأدلة وفقًا للسياق القانوني والتكنولوجي، ولكنها تشترك في تحديده كأداة أساسية في التحقيقات الجنائية لإثبات وقوع الجرائم، سواء كانت الجرائم الرقمية أو التقليدية التي يتم تنفيذها باستخدام التقنيات الحديثة.

الدليل الرقمي في الفقه الجنائي هو المعلومات المخزنة بشكل رقمي عبر أجهزة الحاسوب أو الأجهزة الإلكترونية الأخرى مثل الهواتف المحمولة والأجهزة المتصلة بالشبكات. تتنوع هذه البيانات بين نصوص مكتوبة، صور، أصوات، وفيديوهات، أو أي نوع آخر من المعلومات التي يتم جمعها أو تخزينها باستخدام تقنيات وبرمجيات معينة. يُستخدم هذا النوع من الأدلة في التحقيقات الجنائية لإثبات وقوع الجريمة وربط الجاني بالواقعة، سواء كانت جريمة رقمية كالهجمات الإلكترونية أو جريمة تقليدية تم تنفيذها باستخدام التكنولوجيا الحديثة.

يُعرَّف الدليل الرقمي في بعض المصادر القانونية على أنه المعلومات المخزنة في شكل رقمي عبر الحاسوب، والتي يمكن أن تشمل نصوصًا، صورًا، أو أي بيانات أخرى تم جمعها باستخدام أدوات وتقنيات خاصة. هذه الأدلة تُستخدم في التحقيقات الجنائية لإثبات الجريمة وكشف ملابساتها أو نفيها[77]، وقد يتم جمعها عبر برامج حاسوبية أو تطبيقات الإنترنت . بالإضافة إلى ذلك، يُقدِّم بعض الفقهاء تعريفًا أوسع للدليل الرقمي باعتباره بيانات يمكن إعدادها أو تخزينها رقميًا، حيث تُستخدم هذه البيانات في التحقيقات لتوثيق الجريمة وربط الجاني بالواقعة .

كما ان هناك تعريفات أوسع تشير إلى أن الدليل الرقمي يشمل جميع أنواع المعلومات المخزنة في الأجهزة الإلكترونية، مثل النصوص، الصور، الأصوات والفيديوهات، ويمكن تحليلها باستخدام برمجيات متخصصة. هذه الأدلة تُعَد حاسمة في التحقيقات الجنائية، إذ تساهم في ربط الجريمة بالجاني في بيئات رقمية غير ملموسة. كما تُعرِّف المنظمة الدولية لأدلة الحاسوب (IOCE)الدليل الرقمي على أنه المعلومات المخزنة في شكل ثنائي داخل أنظمة الحاسوب، والتي تُعتمد في المحاكم كأدلة قانونية في القضايا الجنائية[78].

إجمالاً، يُمكن القول أن الدليل الرقمي في القضاء الجنائي هو كل نوع من المعلومات أو البيانات التي يتم جمعها أو تخزينها باستخدام تكنولوجيا المعلومات والاتصالات. يشمل ذلك البيانات المخزنة على أجهزة الحاسوب، الهواتف المحمولة، الخوادم الإلكترونية، الشبكات، أو أي جهاز آخر يستخدم لتخزين أو معالجة المعلومات الرقمية. كما يتضمن المستندات الإلكترونية مثل رسائل البريد الإلكتروني، المحادثات النصية، الصور، مقاطع الفيديو، والبيانات الأخرى التي يتم التقاطها أو معالجتها أو إرسالها عبر وسائل تكنولوجية. ومن ثمة فهو أي نوع من المعلومات الرقمية المخزنة في الأجهزة الإلكترونية، والتي يتم استخدامها لإثبات وقوع الجريمة وارتباطها بالجاني. يشكل هذا الدليل جزءًا أساسيًا من الأدلة الجنائية في العصر الرقمي، ويعتمد جمعه وتحليله على تقنيات متخصصة لضمان دقة المعلومات وقبولها في المحاكم.

ثانيا: خصائص الدليل الرقمي الجنائي :

1) **الطبيعة العلمية والتقنية:** الدليل الإلكتروني الجنائي يتمتع بطبيعة علمية وتقنية بحتة، مما يعني أنه يعتمد بشكل كامل على التكنولوجيا والأنظمة الرقمية. يعتمد جمع الأدلة وتحليلها على أدوات وبرامج متخصصة، مثل برامج تحليل البيانات، وأدوات استرجاع البيانات المفقودة، وبرمجيات تحليل الشبكات. وهذه الأدوات تستند إلى تقنيات علمية مثل تحليل الأنماط

---

[77] - عادل عبد العزيز صالح الرشيد، "قرائن الجريمة الإلكترونية وأثرها في الإثبات "، دار كنوز اشبيليا للنشر والتوزيع، المملكة العربية السعودية 2022، الطبعة الاولى ، ص 70.

[78] - أحمد مسعود مريم، آليات مكافحة الجرائم الإلكترونية في ظل القانون رقم 09-04، مذكرة مقدمة لنيل شهادة الماجستير، منشورة، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2013.

الرقمية، والتشفير، وإجراءات التوثيق الرقمي (مثل التوقيع الإلكتروني والطابع الزمني. هذه الطبيعة التقنية تجعل من الدليل الإلكتروني عنصرًا موثوقًا في التحقيقات الجنائية، حيث يمكن إعادة تحليله باستخدام تقنيات مختلفة للكشف عن تفاصيل قد تكون غير واضحة في التحليل الأولي. لكن في الوقت ذاته، تتطلب هذه الخصائص تقنيات عالية جدًا للتمكن من التعامل مع الأدلة بشكل سليم ومؤثر في سياق القانون.

2) **القابلية للتنوع والتطور**[79]**:** من أبرز خصائص الدليل الإلكتروني الجنائي هو قابليته للتنوع والتطور المستمر. مع تقدم التكنولوجيا، تظهر أنواع جديدة من الأدلة الرقمية تتنوع حسب الوسائل التي يستخدمها المجرمون، مثل الرسائل الإلكترونية، مواقع الإنترنت، البيانات المخزنة على السحابة، أو حتى سجلات المعاملات المالية الرقمية. هذا التنوع لا يقتصر فقط على نوعية البيانات، بل يشمل أيضًا تنوع الوسائط الرقمية (صوت، صورة، فيديو، نصوص) وكذلك تقنيات الاتصال (البريد الإلكتروني، شبكات التواصل الاجتماعي، الرسائل النصية، التطبيقات وغيرها. ومنه يجب على السلطات القضائية أن تواكب هذا التطور التكنولوجي لضمان قبول الأدلة الحديثة في التحقيقات والمحاكمات. ويجب أن تكون القوانين مرنة بما يكفي لاستيعاب الابتكارات التكنولوجية الجديدة والتعامل معها بشكل مناسب.

3) **صعوبة التخلص منه :** من الخصائص الجوهرية للدليل الإلكتروني الجنائي أنه يتمتع بصعوبة كبيرة في التخلص منه أو محوه بشكل كامل، وهذا يعود إلى طبيعة البيانات الرقمية نفسها. فعلى الرغم من أن الملفات قد تُحذف أو تُلغى من الأجهزة، إلا أن آثارها قد تبقى مخزنة في أماكن غير مرئية مثل الذاكرة العشوائية أو الأقراص الصلبة الميتة، بل قد تظل آثارًا من البيانات على أجهزة أخرى قد تم نقلها إليها. إضافة إلى ذلك، يتم عادةً إنشاء نسخ احتياطية من البيانات (على سبيل المثال، من خلال التخزين السحابي أو النسخ الاحتياطية للأجهزة)، مما يجعل من الصعب تمامًا محو كل أثر للمعلومات الرقمية بشكل نهائي. وهذه الخاصية تجعل من الأدلة الإلكترونية موثوقة جدًا في التحقيقات الجنائية، حيث يمكن للمحققين استرجاع المعلومات حتى وإن تم محاولة إخفائها أو محوها. في بعض الأحيان، يتم استخدام تقنيات متقدمة مثل "الاسترجاع الجنائي" لاستعادة البيانات التي تم محوها أو تعديلها.

4) **القابلية للنسخ والإعادة :** من السمات المميزة للدليل الإلكتروني أنه يمكن نسخه بسهولة دون التأثير على أصالته أو جودته. يتيح ذلك للمحققين والمحاكم استخدام نسخ متعددة من الدليل دون التأثير على النسخة الأصلية. هذا يعزز قدرة الدفاع والادعاء على التحليل والمقارنة. بمعنى آخر، يمكن إجراء التحقيقات باستخدام نسخ عديدة من الأدلة، مما يسمح بتكرار التحليل والتأكد من صحة النتائج عبر أوقات وأماكن مختلفة.

رابعا: شروط قبول الدليل الإلكتروني أمام القضاء الجنائي

1. **المشروعية في الحصول على الدليل :** يشترط أن يتم جمع الدليل الإلكتروني بطرق قانونية مشروعة، وفقًا للقواعد القانونية المعمول بها في المجتمع[80]. يجب ألا يتم الحصول عليه عبر طرق غير قانونية مثل اختراق الأنظمة أو التجسس على البيانات، ويجب أن تتماشى إجراءات جمع الأدلة مع القوانين المنظمة للمراقبة والتفتيش.

---

[79] - خالد ممدوح ابراهيم، الاثبات الالكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، الاسكندرية ، 2020، ص 42.

[80] - حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، كلية الحقوق عين شمس، 2005، ص 475 ما بعدها.

2. **سلامة الدليل الإلكتروني وسلامة إجراءات جمعه:** يجب ضمان سلامة الدليل الإلكتروني طوال عملية جمعه وتحليله. على المحققين استخدام أدوات وتقنيات موثوقة تضمن عدم التلاعب بالدليل، مع توثيق كل مراحل جمع الأدلة لضمان مصداقيتها. ينبغي أن يتم حفظ الأدلة في بيئة آمنة لضمان عدم التغيير أو التلاعب بها.

3. **يقينية الدليل الإلكتروني:** يجب أن تكون المعلومات الواردة في الدليل الإلكتروني يقينية قدر الإمكان. لا يجوز أن تعتمد الأدلة الرقمية على الظنون أو التوقعات، بل يجب أن تكون مبنية على معلومات مؤكدة يمكن التحقق منها. أي دليل يتسم بالشكوك أو التخمينات قد يضعف من مصداقيته أمام المحكمة[81].

4. **موثوقية الدليل الإلكتروني:** يجب أن يتمتع الدليل الإلكتروني بمستوى عالٍ من الموثوقية. يتطلب ذلك أن تكون البيانات والملفات المخزنة في الأجهزة الإلكترونية قد تم جمعها باستخدام أدوات وتقنيات دقيقة يمكن الاعتماد عليها. بالإضافة إلى ذلك، يجب أن يكون الدليل الإلكتروني خاليًا من أي تلاعب أو تعديل يؤثر على صحته وموثوقيته.

5. **إثبات حجية الدليل الإلكتروني:** لكي يكون الدليل الإلكتروني مقبولًا أمام القضاء، يجب أن يكون قابلاً للتحقق من صحته ومصدره. يتم إثبات ذلك باستخدام تقنيات مثل التوقيع الإلكتروني والطابع الزمني، التي تساهم في ضمان أصالة الأدلة الرقمية ومنع التلاعب بها. يتعين أن تكون الأدلة متصلة بمصدر موثوق ويمكن تتبعه.

6. **عدم مخالفة الدليل الإلكتروني للضمانات القانونية:** يجب أن يحترم الدليل الإلكتروني الضمانات القانونية المقررة للأفراد، مثل الحق في الخصوصية. جمع الأدلة يجب أن يتم ضمن الإجراءات القانونية الواضحة، مثل الحصول على إذن قضائي لتفتيش الأجهزة الإلكترونية، بحيث لا يؤدي إلى انتهاك الحقوق الدستورية.

7. **ارتباط الدليل بالجريمة:** لا يكفي أن يكون الدليل الإلكتروني صحيحًا من الناحية التقنية، بل يجب أن يكون له علاقة مباشرة بالجريمة محل التحقيق[82]. يجب أن يساهم الدليل في إثبات وقوع الجريمة أو كشف هوية الفاعل، وفي حال عدم وجود صلة واضحة بالجريمة، قد يتم استبعاد الدليل من قبل المحكمة.

8. **قبول القاضي للدليل الإلكتروني وفقًا للسلطة التقديرية:** يتمتع القاضي بسلطة تقديرية واسعة في تقييم الدليل الإلكتروني. فهو غير ملزم بقبول أي دليل إلا إذا اقتنع بصحته وارتباطه بالقضية. يتم تقييم الأدلة الرقمية في سياقها العام ويتم مقارنتها ببقية الأدلة المتاحة قبل أن يتم اتخاذ قرار بشأن قبولها في المحكمة.

ثالثا: طرق جمع الادلة الرقمية الجنائية وموقف المشرع الجزائري منها

يعتمد التحقيق في الجرائم الإلكترونية على مجموعة من الإجراءات التقليدية والحديثة لضمان جمع أدلة سليمة وقابلة للاستخدام في المحكمة. وتنقسم هذه الطرق إلى تقنيات قديمة تعتمد على الأساليب التقليدية، وتقنيات حديثة تستفيد من التقدم التكنولوجي.

أ- الطرق التقليدية لجمع الأدلة الرقمية:

[81] - هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، 1997، ص 91.
[82] - خالد ممدوح ابراهيم، الاثبات الالكتروني في المواد الجنائية والمدنية، المرجع السابق، 46.

1. **الانتقال والمعاينة:** الانتقال هو أحد الإجراءات الأساسية في التحقيقات الجنائية، ويهدف إلى جمع الأدلة وتوثيق الوقائع المرتبطة بالجريمة. يُعتبر الانتقال أداة هامة لفحص وتحليل مسرح الجريمة، ويُنفذ غالبًا عندما تتطلب القضية فحصًا ميدانيًا دقيقًا لتحديد الحقائق والظروف التي قد تكون قد أثرت في وقوع الجريمة. والمعاينة هي عملية فحص ميداني دقيقة تهدف إلى جمع الأدلة المادية التي يمكن أن تكون قد ارتبطت بالجريمة. المعاينة تتضمن "رؤية العين" للمكان أو الشخص أو الشيء المرتبط بالجريمة، بهدف إثبات حالته ومعرفة تفاصيله التي يمكن أن تكون حاسمة في كشف الحقائ[83]ق. ويعد هاذين الاجرائين من أولى الخطوات في جمع الأدلة الرقمية، حيث يتم فحص الأجهزة الإلكترونية مثل الحواسيب والهواتف الذكية والخوادم وغيرها من وسائل التخزين المتصلة بالجريمة. يتم تنفيذ هذه العملية تحت إشراف مختصين معتمدين من قبل السلطات القضائية، وعادة ما يتطلب الأمر إذنًا قضائيًا لتطبيقها. ويقوم المحققون بفحص الأجهزة في مكان الجريمة أو في المواقع المرتبطة بها، بهدف استخراج أي بيانات رقمية تدعم القضية.

2. **الخبرة التقنية:** تتطلب الجرائم الرقمية الاستعانة بالخبراء في علم الحوسبة الجنائية، حيث يتم تحليل الأجهزة والبيانات المخزنة باستخدام أدوات وتقنيات متقدمة. يشمل هذا تحليل الملفات والبرامج المثبتة على الأجهزة الرقمية لاستخراج الأدلة ذات الصلة. المشرع الجزائري منح قاضي التحقيق السلطة الكاملة في اختيار الخبراء وتكليفهم بإجراء الخبرة اللازمة، وذلك وفقًا للمادة 147 من قانون الإجراءات الجزائية. حيث أتاح للقاضي حرية ندب خبير أو أكثر من خبير، وهذا يشمل تكليف خبراء متعددين بحسب نوع القضية واحتياجات التحقيق. وفي هذا السياق، يمكن للقاضي أن يقرر استدعاء مجموعة من الخبراء المتخصصين في مجالات متعددة إذا كانت القضية تتطلب فحصًا من زوايا مختلفة، خاصة في القضايا التي تتطلب خبرات فنية معقدة[84].

3. **التفتيش والضبط:** يعد التفتيش في البيئة الرقمية أحد الإجراءات التقليدية المهمة لجمع الأدلة الرقمية. يشمل هذا التفتيش فحص الأجهزة الرقمية والأنظمة المعلوماتية المشتبه في احتوائها على أدلة مرتبطة بالجريمة. يتم التفتيش عادةً بموجب إذن قضائي، وقد أجاز المشرع الجزائري صراحةً في نص المادة 5 من القانون 09-04 التفتيش في الأنظمة المعلوماتية، مما يعكس إدراكه لأهمية فعالية هذه الأنظمة في مكافحة الجرائم السيبرانية. وبالتالي، يظهر أن المشرع الجزائري قد أخذ بعين الاعتبار الدور الحيوي للأنظمة المعلوماتية في التحقيقات الجنائية، وضرورة تفعيل آليات تفتيش متطورة لهذه الأنظمة في إطار مكافحة الجرائم المرتبطة بالتكنولوجيا.

4. **الشهادة المعلوماتية :** الشاهد في الجرائم المعلوماتية هو شخص ذو خبرة تقنية متخصصة في مجالات الحاسب والشبكات والاتصالات، ويقدّم شهادات فنية بناءً على تحليل الأنظمة الحاسوبية والبيانات الرقمية المتعلقة بالجريمة. يُعتبر الشاهد المعلوماتي مختلفًا عن الشاهد التقليدي نظرًا لأنه لا يشهد بناءً على مشاهداته الشخصية فقط، بل يقدم أدلة فنية من خلال فحص الأنظمة الرقمية واستخراج البيانات ذات الصلة. فئات الشهداء المعلوماتيين تشمل مشغلي الحاسوب الذين يتعاملون مع تشغيل الأجهزة المتصلة، والمبرمجين الذين يكتبون الأكواد البرمجية للبرامج والتطبيقات، والمحللين الذين يقومون بتجميع البيانات وتحليلها لاستنتاج العلاقات بين الوحدات المعلوماتية، إضافة إلى مهندسي الصيانة والشبكات الذين يختصون في صيانة الأنظمة التقنية والاتصالات ...وغيرهم. وقد أخذ المشرع الجزائري بالاتجاه الذي يلزم كل شخص له دراية

---

[83] - عفيفي كمال، "جريمة الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون "، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، ص 303. علي عدنان الفيل "إجراءات التحري في جمع الأدلة والتحقيق الابتدائي في الجرائم المعلوماتية"، دراسة مقارنة، الطبعة الأولى، المكتب الجامعي الحديث، مصر، 2012، ص 22.

[84] - عائشة بن قارة، المرجع السابق، ص 141 و 142.

واطلاع بعمل المنظومات المعلوماتية بمساعدة السلطات المختلفة وتزويدها بكافة المعلومات الضرورية لانجاح مهامها[85].

ب- **الطرق الحديثة لجمع الأدلة الرقمية:**

المشرع الجزائري قام باستحداث أساليب جديدة في التحقيقات الجنائية، اعتُبر بعضها مساسًا بالحياة الخاصة للأفراد، حيث سمحت هذه الأساليب مثل التسجيل الصوتي، التقاط الصور، والتسرب، بكشف الجرائم الإلكترونية. وقد ورد ذلك في المواد (65 مكرر 5 إلى 65 مكرر 18) من قانون الإجراءات الجزائية الجزائري، والتي توفر إطارًا قانونيًا يسمح باستخدام هذه الأساليب لجمع الأدلة الرقمية في التحقيقات في الجرائم الإلكترونية. من بين هذه الأساليب:

1. **اعتراض المراسلات:** اعتراض المراسلات هو إجراء تحقيقي يسمح للسلطات القضائية، وفقًا لشروط محددة قانونيًا، بالتنصت على الاتصالات الخاصة بهدف جمع الأدلة المتعلقة بالجرائم. ويشمل ذلك رسائل البريد الإلكتروني، الرسائل النصية، والمراسلات عبر التطبيقات الرقمية. لم يقدم المشرع الجزائري تعريفًا دقيقًا لهذا الإجراء، بل اكتفى بتنظيمه في المادة (65 مكرر 5) من قانون الإجراءات الجزائية، حيث أجاز في حالات معينة، مثل الجرائم المنظمة، تبييض الأموال، الإرهاب، والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات، اعتراض المراسلات عبر وسائل الاتصال السلكية واللاسلكية. كما يسمح القانون بوضع ترتيبات تقنية لمتابعة المعنيين، بما في ذلك تسجيل المكالمات واعتراض الصور والمحادثات في أماكن خاصة أو عامة، مما يثير التساؤل حول مدى شمولية هذا الإجراء، وهل يقتصر على التنصت الهاتفي فقط أم يمتد إلى وسائل اتصال أخرى، مما قد يمثل مساسًا بالحياة الخاصة للأفراد. وبالرغم من ضرورة الحصول على إذن قضائي مسبق، فإن هذا الإجراء يثير جدلًا قانونيًا حول التوازن بين الأمن وحق الأفراد في الخصوصية.
2. **التقاط الصور :** يعتبر التقاط الصور من الإجراءات الحديثة التي اعتمدها المشرع الجزائري لمكافحة الجرائم الإلكترونية. ويعتمد هذا الإجراء على استخدام الكاميرات والأجهزة الخاصة لالتقاط صور للمشتبه بهم في الجرائم، بهدف استخدامها كأدلة مادية في التحقيقات[86]. ورغم أن المشرع لم يقدم تعريفًا دقيقًا لهذا الإجراء، إلا أنه حدد مجالات تطبيقه باستخدام تقنيات متخصصة لتوثيق الحوادث والجرائم. وقد انتشرت الكاميرات الرقمية في الأماكن العامة والخاصة، مثل البنوك والمطارات والمستشفيات، وذلك لأغراض المراقبة وضبط الجرائم وتوثيق الأدلة. وفي حالات الجرائم، يتم الاطلاع على الصور بعد إصدار أمر قضائي بذلك.
3. **تسجيل الأصوات:** التسجيل الصوتي هو عملية نقل مباشر أو آلي للموجات الصوتية من مصدرها، باستخدام وسائل تقنية خاصة، لحفظها على وسائط تتيح إعادة سماعها لاحقًا. يُستخدم هذا الإجراء في التحقيقات الجنائية بأمر من السلطات القضائية بهدف الحصول على أدلة غير مادية، خاصة في الجرائم الخطيرة. ورغم أهميته في كشف الجرائم، لم يعرّف المشرع الجزائري صراحةً التسجيل الصوتي ضمن قانون الإجراءات الجزائية، لكنه أشار إليه في المادة (65 مكرر) من خلال السماح بوضع ترتيبات تقنية لتسجيل المكالمات بصفة سرية في أماكن

---

[85] - المادة 04/05 من القانون رقم 09-04 الجزائري. رضا هميسي، "أحكام الشاهد في الجريمة المعلوماتية"، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، 17/16 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، 2015، ص 05.

[86] - فوزي عمارة، "اعتراض الممارسات كتسجيل الأصوات والتقاط الصور والتسرب كالإجراءات التحقيقية القضائية في القضايا الجزائية"، مجلة العلوم الإنسانية، العدد 33، 2010، جامعة قسنطينة 1، الجزائر، ص

خاصة أو عامة. ومع ذلك، فإن التسجيلات التي يجريها الأفراد بشكل شخصي دون تدخل قضائي لا تُعد إجراءً جنائيًا، ولا يمكن اعتبارها دليلًا قانونيًا، إلا إذا لم تتضمن اعتداءً على حق الشخص في سرية حديثه، كما هو الحال في تسجيلات البرامج الإذاعية والتلفزيونية والصحفية.

والضوابط التي تحكم إجراءات التقاط الصور وتسجيل الأصوات واعتراض المراسلات تشمل شروطًا شكلية وموضوعية. على المستوى الشكلي، يجب أن تتم هذه الإجراءات تحت إشراف ضابط الشرطة القضائية، بناءً على إذن قانوني من القاضي المختص، ويجب أن يكون الإذن مكتوبًا ويحدد الأشخاص المعنيين، الأماكن المستهدفة، والجريمة التي تبرر اتخاذ هذه التدابير. كما يشترط تحرير محضر تفصيلي يوثق جميع الإجراءات التي تمت. أما على المستوى الموضوعي، فالإجراء لا يتم إلا في حالات خاصة تتعلق بالجرائم التي تستدعي تدخلات مكثفة للتحقيق، مثل الجرائم المرتبطة بأنظمة المعالجة الآلية للبيانات أو الجرائم المنظمة. ويقتصر تنفيذ هذه الإجراءات على ضابط الشرطة القضائية فقط، نظرًا لحساسيتها وتأثيرها المباشر على حرمة الحياة الخاصة للأفراد.

4. **التسرب:** استحدث المشرع الجزائري إجراءات التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية، والتي تنص على أنه: "عندما تقتضي ضرورات التحري او التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 05 من هذا القانون، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب وفق الشروط المبينة في المواد ادناه".

وقد حدد المشرع الجزائري تعريف التسرب، في نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية، والتي تنص على: "يقصد بالتسرب قيام ضابط الشرطة القضائية، أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم لجناية أو جنحة بايهامهم انه فاعل معهم او شريك لهم او خاف. ويسمح لضابط او عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة أو أن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 ولا يجوز تحت طائلة البطلان ان تشكل هذه الأفعال تحريضا على ارتكاب جرائم".

وإجراء التسرب، مثل باقي الإجراءات الحديثة، يخضع لضوابط شكلية وموضوعية دقيقة لضمان مشروعيته وقانونيته. على الصعيد الشكلي، يُلزم ضابط الشرطة القضائية المكلف بالتسرب بتحرير تقرير كتابي شامل يتضمن ترتيبًا زمنيًا دقيقًا لكافة الأحداث والإجراءات المتخذة منذ بداية العملية حتى نهايتها، مع تحديد الأشخاص المشتبه بهم وشرح كيفية إخفاء هويتهم. كما يجب الحصول على إذن كتابي من القاضي المختص، بعد إخطار النيابة العامة، يشير بوضوح إلى الجريمة التي تبرر التسرب ومدة العملية. وفقًا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية، لا تتجاوز مدة التسرب أربعة أشهر، ويمكن تمديدها إذا استدعت الحاجة وفقًا لمقتضيات التحقيق. أما على الصعيد الموضوعي، فيشترط أن يكون هناك تسبيب واضح للإذن بالتسرب، حيث يجب أن يوضح القاضي أو ضابط الشرطة القضائية الأدلة والشهادات التي تبرر اتخاذ هذا الإجراء، مع تقديم تقييم دقيق للمعطيات ذات الصلة بالقضية. كما أن الجريمة التي تبرر التسرب يجب أن تكون من الجرائم المحددة في المادة 65 مكرر 5 من قانون الإجراءات الجزائية، والتي تشمل الجرائم مثل المخدرات، الجريمة المنظمة العابرة للحدود، الجرائم التي تمس بأنظمة المعالجة الآلية للبيانات، تبييض الأموال، الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرامة، والفساد.

وبالتالي، فإن التسرب لا يُسمح به إلا في حالة الجريمة المرتبطة بهذه الأنواع، سواء كانت جناية أو جنحة.

5- **مراقبة الاتصالات الإلكترونية :** لم يتطرق المشرع الجزائري بشكل مفصل إلى تعريف "مراقبة الاتصالات الإلكترونية"، لكن بالمقابل، وضح لنا مضمون الاتصالات الإلكترونية في المادة 02 من القانون رقم 09-04 والتي تنص على: "يقصد في هذا القانون ما يلي: الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو شارات أو كتابات أو صور أو أصوات أو أية معلومات مختلفة بواسطة أي وسيلة الكترونية وبذلك وسع المشرع الجزائري مفهوم الاتصالات الالكترونية ليشمل كافة الوسائل الحديثة مثل أجهزة الفاكس وغيره من الأنظمة الإلكترونية الأخرى.

ويمكن تعريف مراقبة الاتصالات الإلكترونية بأنها "العملية التي يقوم فيها المراقب باستخدام الوسائل الإلكترونية لجمع المعطيات المتعلقة بالأشخاص المشتبه بهم، سواء كان ذلك لجهة مكانهم أو نشاطاتهم، مثل مراقبة الأشخاص باستخدام الكمبيوتر الشخصي أو إعداد بريد إلكتروني مستنسخ لمراقبة المشتبه فيهم.

حالات اللجوء إلى مراقبة الاتصالات الإلكترونية: من غير شك، تعتبر مراقبة الاتصالات الخاصة عبر وسائل الاتصال الإلكتروني مسألة تمس بالخصوصية، وهو ما يتطلب توازنًا دقيقًا في التشريعات الحديثة، التي تهدف إلى حماية الحقوق الفردية في هذا المجال. وفي هذا السياق، نصت المادة 04 من القانون 09-04 على الحالات التي يجوز فيها تنفيذ مراقبة الاتصالات الإلكترونية، وهي كالتالي:

-**لمكافحة الجرائم الإرهابية والتخريبية** :عندما تتعلق الأفعال المرتكبة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بالأمن الوطني.
-**في حالة الاعتداء على الأنظمة المعلوماتية** :عند احتمال حدوث هجوم على أنظمة المعلومات الخاصة بالحكومة أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
-**في إطار التحقيقات القضائية** :عندما تتطلب التحقيقات القضائية بالضرورة متابعة العمليات الإلكترونية للكشف عن الجرائم.
-**تنفيذ طلبات المساعدة القضائية الدولية** :في حال طلب المساعدة من الدول الأخرى في إطار التحقيقات الدولية.

ولا يجوز اتخاذ إجراءات المراقبة في الحالات المذكورة أعلاه إلا بعد الحصول على إذن من السلطة القضائية المختصة.

6- تفتيش المنظومة المعلوماتية وحجزها: بموجب المادة 5 من القانون 09-04، يمكن للسلطات القضائية وضباط الشرطة القضائية إجراء التفتيش على الأنظمة المعلوماتية، بما في ذلك التفتيش عن بُعد على البيانات المخزنة داخل هذه الأنظمة. إذا كانت المعطيات المبحوث عنها موجودة في نظام معلوماتي يقع خارج حدود الجزائر، يتم الحصول عليها بمساعدة السلطات الأجنبية المختصة. ومن أجل تسهيل هذا التفتيش، يمكن للسلطة المكلفة بالتحقيق الاستعانة بخبراء في الأنظمة المعلوماتية أو بمن يمتلكون المعرفة اللازمة لضمان سلامة المعطيات وحمايتها.

ووفقا للمادة 06 من ذات القانون عندما يتم اكتشاف معطيات تخدم التحقيق وتساعد في الكشف عن الجرائم أو الجناة، يتم نسخ المعطيات المحفوظة التي تتعلق بالقضية أو المهمة الجنائية على وسائط تخزين إلكترونية، والتي يتم بعد ذلك حجزها وفقاً للقواعد المعمول بها في قانون الإجراءات الجزائية. ولا يسترط ان يتم حجز كامل النظام المعلوماتي، بل فقط المعطيات التي تتعلق بالتحقيق، والتي يتم نسخها وحجزها بشكل يمكن معه الرجوع إليها لاحقاً. كما يجب على السلطة التي تقوم بالتفتيش أن تضمن الحفاظ على سلامة النظام المعلوماتي المعني. ويجوز لها استخدام الوسائل والتقنيات اللازمة لضمان عدم تلف أو تعديل المعطيات أثناء عملية الحجز أو التفتيش. كما يشدد القانون على أن استخدام التقنيات لإعادة تشكيل المعطيات يجب ألا يؤثر على محتوى هذه المعطيات أو يعرضها للتلاعب.

الفرع الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي

تعد الأدلة الإلكترونية من الوسائل الحديثة التي غزت النظام القضائي في العديد من الدول، بما في ذلك الجزائر. وقد أصبح لهذه الأدلة دور كبير في إثبات الجرائم الجنائية، خاصة في ظل تطور التقنيات الحديثة. لكن على الرغم من أهميتها، يظل قبول هذه الأدلة في القضاء مرهونًا بجملة من الشروط القانونية التي تتفاوت باختلاف الأنظمة القضائية. وفيمايلي يتم دراسة أنظمة الاثبات وموقف المشرع الجزائري منها ، وسلطة القاضي الجنائي في تقدير الدليل الالكتروني.

أولا: أنظمة الإثبات الجنائي وموقف المشرع الجزائري منها

تختلف الأنظمة القانونية في كيفية التعامل مع الأدلة الإلكترونية في الإثبات الجنائي، ويُعد التمييز بين **الأنظمة الحرة** و **الأنظمة المقيدة** في قبول الأدلة أمرًا بالغ الأهمية.

1- في ظل نظام الإثبات الحر

في نظام الإثبات الحر، يُمنح القاضي الجنائي حرية واسعة في تقدير الأدلة الرقمية، بما في ذلك الأدلة الإلكترونية مثل سجلات الكمبيوتر، الرسائل الإلكترونية، والبيانات الرقمية الأخرى. لا يخضع تقدير القاضي لرقابة المحكمة العليا، لكنه ملزم باتباع معايير منطقية تبرر قبوله للأدلة الرقمية. القاضي في هذا النظام يتحمل المسؤولية كاملة في تقييم قيمة الأدلة ومدى صلاحيتها.

تتبع بعض التشريعات مثل **فرنسا** و**تركيا** و**إيطاليا** هذا النظام، حيث تعتبر الأدلة الرقمية مقبولة طالما تم جمعها بطرق قانونية. وفي بعض الحالات مثل **فرنسا**، يشترط أن تكون الأدلة قد تم جمعها باستخدام وسائل قانونية، مثل الحصول على البيانات من الخوادم أو الأجهزة عبر إذن قضائي. في هذا السياق، يقوم القاضي بتقييم الأدلة وفقًا للمعايير القانونية والمهنية، وغالبًا ما يتم الاستعانة بالخبراء لتوضيح مدى قوة الأدلة الإلكترونية وفهمها في القضية.

2- في ظل نظام الإثبات المقيد

في النظام المقيد، لا يُترك للقاضي كامل الحرية في تقدير الأدلة الرقمية، بل يتم تحديد الأدلة المقبولة وفقًا للمعايير التي يحددها المشرع. هذا النظام يتطلب وجود معايير دقيقة وواضحة للأدلة الإلكترونية التي يمكن قبولها، ويهدف إلى ضمان جمع الأدلة بطريقة قانونية وأخلاقية.

تُعد **المملكة المتحدة** و**الولايات المتحدة** من أبرز الدول التي تتبنى النظام المقيد، حيث يشترط القانون أن يتم الحصول على الأدلة الرقمية وفقًا لمعايير قانونية دقيقة، مثل مبدأ **تعاضد الأدلة** الذي يتطلب وجود دليل مادي آخر يعزز الأدلة الرقمية. كما يشترط **القانون الألماني** في بعض الحالات أن تتضمن الأدلة الرقمية شهادة خبير مختص، ويستبعد الأدلة التي تم جمعها بطرق غير قانونية مثل التفتيش أو المصادرة غير المصرح بها.

في النظام المقيد، يمكن قبول الأدلة الرقمية فقط إذا كانت قد تم جمعها بشكل قانوني وبالتوافق مع المعايير القانونية المحددة. إذا كان هناك أي تناقض بين الأدلة وجمعها بطريقة غير قانونية، يتم رفضها من قبل المحكمة. وهذا النظام يهدف إلى حماية حقوق الأفراد وضمان أن الأدلة الرقمية المرفوعة أمام المحكمة تم جمعها بشكل قانوني ومشروع.

3- في ظل نظام الإثبات المختلط

النظام المختلط للإثبات هو مزيج من النظامين الحر والمقيد، حيث يتمتع القاضي بحرية تقدير الأدلة الرقمية لكن ضمن قيود قانونية تحرص على ضمان نزاهة الإجراءات القانونية. يُمكن في هذا النظام استخدام الأدلة الرقمية طالما أنها تتوافق مع المعايير القانونية، ولكن يتم تحديد نوع الأدلة المقبولة ومتى يمكن استخدامها.

اليابان هي إحدى الدول التي تتبنى هذا النظام، حيث يُسمح باستخدام الأدلة الرقمية وفقًا لمعايير قانونية محددة، لكن مع وضع ضوابط واضحة للأدلة المقبولة. في هذا النظام، يُتاح للقاضي تقدير الأدلة الرقمية بشرط أن تتماشى مع القوانين المعمول بها.

4- موقف المشرع الجزائري من أنظمة الإثبات الجنائي

نظام الإثبات الجنائي في الجزائر يعتمد بشكل عام على نظام الإثبات المختلط، حيث يجمع بين المرونة في تقدير الأدلة ووجود شروط قانونية واضحة لضمان حماية الحقوق وحسن استخدام الأدلة، وخاصة في القضايا الجنائية. هذا التوجه يمكننا فهمه من خلال المادة 212 من قانون الإجراءات الجزائية، والتي تسمح للقاضي الجنائي بالتقدير الحر للأدلة، ما عدا في الحالات التي يُنص فيها القانون على غير ذلك. إذ تنص المادة على أنه يمكن إثبات الجرائم بأي طريقة من طرق الإثبات، باستثناء الحالات التي يُحدد فيها القانون طرقًا معينة. ومع ذلك، فإن القاضي الجنائي لا يُسمح له بأن يبني حكمه إلا على الأدلة المقدمة في المرافعات والتي تم مناقشتها حضوريًا أمامه. هذا يُظهر أن الحرية في تقدير الأدلة تظل مقيدة بإطار قانوني يسمح فقط للأدلة المعتمدة رسميًا في المحاكمة.

لكن، رغم هذه الحرية في التقدير، فإن المشرع الجزائري لا يعتمد على الإثبات الحر المطلق في جميع المجالات. خاصة عندما يتعلق الأمر بالأدلة الرقمية في القضايا الجنائية. فالمشرع الجزائري يتبنى نظام الإثبات المختلط في هذا السياق، حيث يُسمح باستخدام الأدلة الرقمية في المحاكمات الجنائية، ولكن تحت شروط قانونية صارمة .يتضح ذلك في القانون 09-04 المتعلق بحماية البيانات الشخصية، الذي ينظم كيفية جمع الأدلة الرقمية ويشترط أن يتم التفتيش على الأنظمة المعلوماتية بموافقة السلطات القضائية المختصة. وبالتالي، تُفرض قيود صارمة على كيفية

جمع الأدلة الرقمية لضمان أنها تمت وفقًا للقانون، مما يضمن احترام حقوق الأفراد وحمايتهم من أي انتهاك لخصوصيتهم.

إن موقف المشرع الجزائري من أنظمة الإثبات الجنائي الرقمي يتجسد في توازن دقيق بين الحرية القانونية في تقدير الأدلة وضرورة الامتثال للضوابط القانونية المتعلقة بكيفية جمع الأدلة، خاصة الأدلة الرقمية .ورغم أن المادة 212 من قانون الإجراءات الجزائية تمنح القاضي الجنائي حرية تقدير الأدلة، إلا أن المشرع الجزائري يفرض قيودًا قانونية على نوع الأدلة المقبولة، بما في ذلك الأدلة الرقمية التي يجب أن تُجمع بموافقة قضائية وتحت إشراف دقيق لضمان حماية الخصوصية وحقوق الأفراد.

ثانيا: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني

يتمتع القاضي الجنائي وفق المشرع الجزائري بحرية واسعة في تقدير الأدلة الإلكترونية كما هو الحال مع الأدلة التقليدية الأخرى. ومع ذلك، تبقى هذه السلطة مشروطة بالمعايير القانونية التي تضمن نزاهة المحاكمة وحقوق الأطراف.

سلطة القاضي الجنائي في تقدير الدليل الإلكتروني

تعتبر **سلطة القاضي الجنائي** في تقدير الأدلة الإلكترونية واحدة من أبرز التحديات القانونية التي تواجه المحاكم في العصر الرقمي. إذ تزداد أهمية هذه الأدلة في القضايا الجنائية المتعلقة بالجرائم الإلكترونية، حيث يمكن أن تكون الأدلة الرقمية هي العنصر الأساسي في إثبات الجريمة أو البراءة. وفي هذا السياق، يمتلك القاضي الجنائي، كما في معظم النظم القانونية، **سلطة تقديرية** واسعة لتقييم الأدلة المقررة في الدعوى الجنائية، بما في ذلك الأدلة الإلكترونية.

.1امبدأ الاقتناع الشخصي للقاضي الجنائي في تقدير الأدلة الالكترونية

مبدأ الاقتناع الشخصي للقاضي الجنائي يعني أن القاضي هو الذي يقرر مدى صحة وكفاية الأدلة المقدمة أمامه، بناءً على تقديره الخاص. يتيح هذا المبدأ للقاضي حرية تامة في تفسير الأدلة والتوصل إلى القناعة التي تبرر حكمه، دون أن يكون ملزمًا بتوضيح آلية تفكيره. هذا المبدأ مكرس في **المادة 212** من قانون الإجراءات الجزائية الجزائري، التي تنص على أن القاضي يصدر حكمه بناءً على اقتناعه الشخصي، ولا يُلزم بتفسير وسيلة وصوله إلى هذا الاقتناع[87]. كما أن **المادة 307** تؤكد على أن القاضي لا يُطلب منه تقديم حساب حول الوسائل التي بها وصل إلى قناعته، بل يجب عليه أن يضع ضميره نصب عينيه عند تقدير الأدلة[88].

---

[87] - يجوز اثبات الجرائم باي طريق من طرق الاثبات ما عدا الاحوال التي ينص فيها القانون على غير ذلك وللقاضي ان تصدر حكمه تبعا لاقتناعه الخاص ولا يصوغ للقاضي ان يبني قراره الا على الادله المقدمه له في معرض المرافعات والتي حصلت المناقشه فيها حضوريا امامه

[88] - الماده 307يتلو الرئيس قبل مغادره المحكمه قاعه الجلسه التعليمات الاتيه التي تعلق فضلا عن ذلك بحروف كبيره في اظهر مكان من غرفه المداوله ان القانون لا يطلب من القضاه ان يقدموا حسابا عن الوسائل التي بها قد وصلوا الى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم ان يخضعوا لها على الاخص تقدير تمام او كفايه دليل ما ولكنه يامرهم ان يسالوا انفسهم في صمت وتدبر وان يبحثوا باخلاص ضمائرهم في اي تاثير قد احدثته في ادراكهم الادله المسنده الى المتهم واوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم هل لديكم اقتناع شخصي

بخصوص الأدلة الرقمية، يظل القاضي الجنائي في الجزائر هو صاحب القرار النهائي في تقييم الأدلة الإلكترونية، بشرط أن تكون قد تم جمعها بطريقة قانونية. المشرع الجزائري يتبنى **نظام الإثبات المختلط**، الذي يسمح للقاضي باستخدام الأدلة الرقمية وفقًا لشرط جمعها بشكل قانوني، مع ضمان حماية حقوق الأفراد. ومع ذلك، يظل القاضي الجنائي يعتمد على تقديره الشخصي في قبول هذه الأدلة، وفقًا لمعاييره الخاصة، كما هو منصوص عليه في المادة 212، حيث لا يُبنى القرار إلا على الأدلة التي تم مناقشتها أمامه بشكل علني ووفقًا للأصول القانونية.

.2ضوابط سلطة القاضي في تقدير الأدلة الإلكترونية:

على الرغم من أن القاضي الجنائي يمتلك حرية تقدير الأدلة، إلا أن هناك عدة ضوابط تلتزم بها المحكمة لضمان العدالة وحقوق الأفراد:

- **قانونية جمع الأدلة** :كما ينص قانون 09-04 المتعلق بحماية البيانات الشخصية، يجب أن يكون جمع الأدلة الإلكترونية قد تم بطريقة قانونية وسليمة. فعلى القاضي التأكد من أن الأدلة تم جمعها بموافقة السلطة القضائية المختصة وبمراعاة الإجراءات القانونية المقررة لحماية الخصوصية وحقوق الأفراد.
- **حماية الحقوق الأساسية** :يُشترط على القاضي أن يراعي عدم انتهاك حقوق الأفراد خلال جمع الأدلة أو استخدامها. فالاعتداء على حقوق الخصوصية، أو الحصول على الأدلة الإلكترونية بطريقة غير قانونية، مثل التسلل إلى الحسابات أو الأجهزة، يجعل الأدلة غير مقبولة. على القاضي فحص جميع هذه الجوانب قبل اتخاذ أي قرار.
- **الاعتماد على الخبراء** :نظرًا للجانب التقني المعقد للأدلة الإلكترونية، قد يحتاج القاضي إلى الاستعانة بخبراء متخصصين في الحوسبة الجنائية لتوضيح كيفية جمع الأدلة وصحتها. ويصبح الرأي الفني لهؤلاء الخبراء حاسمًا في تفسير الأدلة الرقمية وتقديم تقرير موضوعي يوضح مدى صحتها واستخدامها.

المبحث الثاني: دور تكنولوجيات الإعلام والاتصال في تأمين أدلة الإثبات القانونية: التصديق والحفظ الإلكترونيين

في ظل التحولات التكنولوجية المتسارعة التي يشهدها العالم، أصبح من الضروري أن تتبنى الأنظمة القانونية أساليب جديدة وفعّالة للتعامل مع الأدلة في مختلف القضايا القانونية. تكنولوجيا الإعلام والاتصال، التي تشمل العديد من الأدوات الرقمية مثل الإنترنت والحواسيب والهواتف الذكية، قد أسهمت بشكل كبير في تطوير آليات جمع، تخزين، وتحليل الأدلة القانونية، ما يساهم في تعزيز العدالة وسرعة الفصل في القضايا.

يعد التصديق الإلكتروني والحفظ الإلكتروني من أبرز التقنيات التي أسهمت في تأمين الأدلة القانونية. حيث يتيح التصديق الإلكتروني ضمان صحة الوثائق والبيانات التي يتم تبادلها رقميًا، مما يرفع من مستوى الثقة في الأدلة المقدمة أمام المحاكم. من جهة أخرى، يلعب الحفظ الإلكتروني دورًا حيويًا في تأمين الأدلة ضد التلاعب أو الفقدان، عبر تخزينها في بيئة آمنة وسهلة الوصول.

تهدف هذه الدراسة إلى استكشاف دور تكنولوجيات الإعلام والاتصال في تأمين أدلة الإثبات القانونية، مع التركيز على آلية التصديق الإلكتروني وطرق الحفظ الإلكتروني. سيتم تحليل كيفية

استفادة الأنظمة القانونية من هذه الأدوات لضمان مصداقية الأدلة الرقمية، فضلاً عن مناقشة التحديات التي قد تطرأ في هذا السياق. كما سنستعرض القواعد القانونية التي تحكم استخدام هذه التقنيات، بما يضمن حماية حقوق الأطراف ويعزز من فعالية الإجراءات القضائية في العصر الرقمي.

المطلب الاول : التصديق الإلكتروني ودوره في تعزيز حجية الإثبات المدني الرقمي

يُعد التصديق الإلكتروني أحد الآليات الأساسية التي جمعت بين التكنولوجيا والقانون لضمان الثقة والموثوقية في المعاملات الإلكترونية. يتطلب التصديق الإلكتروني التحقق من هوية الأطراف، والتأكد من صحة إرادتهم، ونسبة التوقيعات الإلكترونية إليهم في سياق غياب الاتصال المباشر بينهم. وتستخدم تكنولوجيات الإعلام والاتصال الحديثة، مثل الإنترنت والتقنيات الرقمية، في توفير البنية التحتية اللازمة لإتمام هذه المعاملات بطريقة آمنة وموثوقة.

وقد أسندت القوانين الإقليمية والوطنية، بما في ذلك التشريع الجزائري، مهمة التصديق الإلكتروني إلى هيئات تُعرف بـ"مؤدي خدمات التصديق الإلكتروني"، التي تقوم بدور الطرف الثالث الموثوق لتوثيق التعاملات الرقمية. تُصدر هذه الهيئات شهادات تصديق إلكتروني تؤكد هوية الأطراف المتعاقدة وصلاحيتهم القانونية. ويستدعي تنظيم هذه الهيئات وجود إطار قانوني دقيق يُحدد شروط الترخيص لها، والتزاماتها، ومسؤولياتها، بالإضافة إلى تنظيم شهادات التصديق التي تصدر عنها، بما لها من دور حاسم في ضمان حجية الكتابة والتوقيع الإلكترونيين المصادق عليهما.

في هذا السياق، تعتمد التشريعات المتعلقة بالإثبات الإلكتروني، ومنها التشريع الجزائري، على آلية "التصديق الإلكتروني" كأساس للاعتراف بالتوقيع والكتابة الإلكترونية ومنحهما الحجية القانونية. يتطلب التصديق الإلكتروني استيفاء معايير فنية وقانونية دقيقة لضمان موثوقيتهما، ويُعتمد على التشفير الإلكتروني كعنصر أساسي لإنشاء توقيعات إلكترونية آمنة. حيث يقوم مقدم خدمات التصديق بإصدار مفاتيح تشفير خاصة بكل مستخدم، مما يعزز الأمان ويؤكد مصداقية المعاملات الرقمية. لذلك، فإن تكنولوجيات الإعلام والاتصال تشكل أساس العملية، بينما يُعد التصديق الإلكتروني أداة قانونية وتقنية أساسية لضمان حماية المعاملات الرقمية وتأكيد صحتها.

من خلال هذه العلاقة بين تكنولوجيا الإعلام والاتصال والتصديق الإلكتروني، تمكّن المشرعين من وضع تشريعات تدعم عملية التصديق وتحمي التوقيعات والكتابات الإلكترونية من أي تلاعب، مع ضمان كفاءة وموثوقية التعاملات الإلكترونية في عالم يتزايد فيه الاعتماد على التكنولوجيا في مختلف المجالات.

الفرع الاول: تعريف التصديق الالكتروني

تتباين تسميات الآلية القانونية التقنية التي تمنح التوقيع والكتابة الإلكترونية الحجية القانونية بين التشريعات، حيث تستخدم بعض القوانين مصطلح "التصديق الإلكتروني (la certification électronique)"[89]، بينما تُفضل أخرى مصطلح "التوثيق الإلكتروني"[90] (l'authentification)

[89]- ونذكر من هذه التشريعات: قانون الاونسترال النموذجي بشان التوقيعات الالكترونية لعام 2001، المرسوم الفرنسي رقم 2001-272 الصادر ب 30 مارس 2001، قانون التوقيع والتصديق الالكترونيين الجزائري رقم 15-04، و القانون

électronique).ورغم هذا الاختلاف الاصطلاحي[91]، فإن الفقه القانوني متفق على جوهر المعنى، والذي يتمثل في آلية تضمن التحقق من هوية مصدر التوقيع أو الكتابة الإلكترونية، وتثبت نسبتهما إليه ورضاه بمحتواهما، بالاعتماد على شهادة إلكترونية موثوقة تستوفي متطلبات قانونية وفنية محددة.

وقد قدم الفقه عدة تعريفات للتصديق الإلكتروني[92]، أبرزها اعتباره وسيلة فنية آمنة يتم تنفيذها من قبل جهة معتمدة أو طرف ثالث محايد، للتحقق من صحة التوقيع أو المحرر الإلكتروني ونسبته إلى صاحبه، والتأكد من سلامة مضمون المعاملة الإلكترونية. وتُسند هذه المهام عادة إلى جهات يُطلق عليها مقدمو خدمات التصديق الإلكتروني. كما أن التعريفات التقنية، سواء من المعهد الوطني الأمريكي للعلوم والتكنولوجيا أو من المنظمة الدولية للتقييس(ISO) ، تركز على أن التصديق هو إجراء يهدف إلى خلق الثقة في هوية المستخدم ومطابقة الأنظمة لمعايير محددة، بما يضمن سلامة التعاملات الإلكترونية [93]وحمايتها.

المشرع الجزائري لم يعرف التصديق الإلكتروني بشكل مباشر، بل اكتفى بتعريف شهادة التصديق الإلكتروني. وفقًا للمادة (7/2) من قانون التوقيع والتصديق الإلكترونيين رقم 15-04، يتم تعريف شهادة التصديق الإلكتروني على أنها وثيقة تثبت العلاقة بين بيانات التحقق من التوقيع الإلكتروني والموقع. كما نصّ في المادة 06 من القانون رقم 15-03 المتعلق بعصرنة العدالة على أن العلاقة بين معطيات التحقق من التوقيع الإلكتروني وصاحب التوقيع تُثبَت من خلال شهادة إلكترونية موصوفة تصدرها وزارة العدل. ومن خلال هذه التعريفات، يمكن استنتاج أن التصديق الإلكتروني هو الآلية التي تتيح التحقق من صحة البيانات الإلكترونية للتوقيع والكتابة الإلكترونية وتحديد هوية صاحبها، إلا أن المشرع الجزائري ركز في تعريفه على شهادة التصديق بدلاً من تعريف التصديق الإلكتروني بشكل مستقل.

كما تعرض التنظيم الاوروبي رقم 910-2014 الصادر بتاريخ 23 جويلية 2014، لمفهوم "التوثيق" بموجب المادة 05/03 منه، والتي اعتبرت بأنّه:"عملية إلكترونية تسمح بالتحقق من هوية شخص طبيعي أو معنوي أو أصل وسلامة معطى ما"، وتعريف كهذا لا يقصر التوثيق أو

التونسي للمبادلات والتجارة الالكترونية التونسي رقم 83 لسنة 2000، أخذ بتسمية" المصادقة الالكترونية" هو كترجمة لتسمية :"certification électronique" التي أخذ بها المشرع الفرنسي في المرسوم الفرنسي رقم 272-2001 الصادر ب 30 مارس 2001.

[90]- ومنها على وجه الخصوص التنظيم الاوروبي رقم 910-2014 الصادر عن البرلمان الاوروبي في 23 جويلية 2014 المتعلق بتحديد الهوية الالكترونية وخدمات الثقة في المعاملات الالكترونية وقانون المعاملات الإلكترونية الاردني رقم 15 لسنة 2015.

[91] - يرى بعض الفقهاء أن استخدام مصطلح "التصديق الإلكتروني" قد يسبب التباسًا مع مفهوم "التصديق الرسمي" المعتمد في بعض الأنظمة القانونية، والذي يعني قيام موظف مختص بالمصادقة على توقيعات الأفراد بإضافة توقيعه وختمه الرسمي لإثبات الهوية وتاريخ العقد دون التدخل في مضمونه. لذلك، يفضل البعض استعمال مصطلحات بديلة مثل "التوثيق الإلكتروني" أو "التعريف الإلكتروني" أو حتى "الاستشهاد الإلكتروني"، لتفادي هذا الخلط وإبراز الطابع التقني والرقمي لهذا النوع من التصديق.

[92] - آلاء احمد محمد حاج علي، التنظيم القانوني لجهات التصديق الالكتروني، أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجيستير في القانون الخاص، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس، فلسطين، 2013، ص 29 و30.

[93] - فؤاد علي البحراني، الإطار العام للتصديق الإلكتروني، ورقة للمناقشة حول الإطار العام لأمن المعلومات الوطني، الجهاز المركزي لتكنولوجيا المعلومات، فبراير 2008، ص 01.

التصديق الالكتروني على عملية التحقق والتثبت من الهوية الالكترونية للأشخاص، بل يمتد كذلك للتحقق من صحة أصل وسلامة البيانات الإلكترونية.

الفرع الثاني: النظام لمؤدي خدمات التصديق الالكتروني

أسوةً بالتنظيم الأوروبي والتشريعات الدولية، وضع المشرع الجزائري قواعد قانونية محددة لتنظيم التصديق الإلكتروني ومؤديه، وذلك بهدف ضمان موثوقية المعاملات الإلكترونية وحمايتها من التلاعب. يتناول هذا النظام تحديد ماهية الهيئات المسؤولة عن تقديم خدمات التصديق الإلكتروني، والشروط التي يجب توافرها لمنحها الترخيص لمزاولة هذه الخدمات. كما يحدد القواعد التي تنظم نشاط هذه الهيئات، بما في ذلك واجباتها ومسؤولياتها لضمان صحة البيانات والهوية في المعاملات الإلكترونية، بما يعزز الثقة في البيئة الرقمية ويضمن الأمن السيبراني.

أولا: التعريف بمؤدي خدمات التصديق الالكتروني:

تناول القانون الجزائري رقم 15-04 في مادته (12/2) تعريف "مؤدي خدمات التصديق الإلكتروني" بأنه "شخص طبيعي أو معنوي يقوم بمنح شهادات تصديق إلكتروني موصوفة، وقد يقدم خدمات أخرى في مجال التصديق الإلكتروني". يركز هذا التعريف على دور الهيئات المختصة في إصدار شهادات التصديق الإلكتروني التي تثبت هوية الأفراد وتوثق صحتها في المعاملات الإلكترونية.

أما التنظيم الأوروبي رقم 910-2014 الصادر في 23 يوليو 2014، فقد قدم تعريفًا موسعًا في مادته (19/3) حيث نص على أن "مقدم خدمات الثقة هو شخص طبيعي أو معنوي يقدم خدمة أو أكثر من خدمات الثقة، ويمكن أن يكون موصوفًا أو غير موصوف". وتُعرّف "خدمة الثقة" في الفقرة 16 من نفس المادة على أنها "خدمة إلكترونية تقدم عادة مقابل مالي وتتمثل في إنشاء والتحقق من التوقيعات الإلكترونية، الأختام الإلكترونية، الطوابع الزمنية الإلكترونية، خدمات الإرسال الموصى عليه إلكترونيًا، بالإضافة إلى الشهادات المتعلقة بهذه الخدمات، وأيضًا إنشاء والتحقق من الشهادات لأجل توثيق مواقع الإنترنت، أو حفظ التوقيعات الإلكترونية والأختام الإلكترونية والشهادات ذات الصلة."

يتضح من مقارنة التعريفين أن القانون الجزائري يركز بشكل أساسي على دور "مؤدي خدمات التصديق الإلكتروني" في إصدار شهادات التصديق الإلكتروني التي تُستخدم للتحقق من صحة التوقيعات الإلكترونية والهوية، مع إمكانية تقديم خدمات أخرى ذات صلة. بينما التنظيم الأوروبي يقدم تعريفًا أوسع لمقدمي خدمات الثقة، حيث يشمل عدة خدمات متكاملة تهدف إلى ضمان أمان الوثائق والبيانات الإلكترونية عبر التوقيعات الإلكترونية، الأختام والطوابع الزمنية، توثيق المواقع الإلكترونية، وحفظ الشهادات المتعلقة بها.

ثانيا: شروط ممارسة نشاط التصدق الالكتروني

وضعت التشريعات الجزائرية شروطًا محددة لتنظيم تقديم خدمات التصديق الإلكتروني، بهدف ضمان موثوقية هذه الخدمات وتعزيز الأمان في التعاملات الإلكترونية. وفقًا لقانون التوقيع والتصديق الإلكتروني رقم 15-04، يُشترط أن يحصل أي شخص يرغب في تقديم خدمات التصديق الإلكتروني على ترخيص مسبق من الهيئة المختصة. ويهدف هذا الشرط إلى ضمان

الرقابة المسبقة على النشاط والتحقق من توافر الشروط اللازمة لممارسته. وتنص المادة 33 من القانون على أن "يخضع نشاط تأدية خدمات التصديق الإلكتروني إلى ترخيص تمنحه السلطة الاقتصادية للتصديق الإلكتروني"، وهي الجهة المسؤولة عن ضبط البريد والمواصلات السلكية واللاسلكية في الجزائر.

حدد المشرع الجزائري في المادة 34 من نفس القانون مجموعة من الشروط التي يجب أن تتوافر في الأشخاص الراغبين في تقديم خدمات التصديق الإلكتروني. وتتمثل هذه الشروط في متطلبات شخصية وفنية تهدف إلى ضمان موثوقية وأمان الخدمة المقدمة. على المستوى الشخصي، يشترط أن يكون الشخص الطبيعي جزائري الجنسية، بينما يجب أن يخضع الشخص المعنوي للقانون الجزائري. كما يجب أن يمتلك مقدم الخدمة القدرة المالية اللازمة لممارسة النشاط، وأن يكون قد حصل على سجل قضائي نظيف خالٍ من الجرائم أو الجنح التي تتعارض مع نشاط التصديق الإلكتروني. علاوة على ذلك، يشترط أن يتمتع مقدم الخدمة أو المسؤول عن المؤسسة بالخبرة الكافية في مجالات تكنولوجيا المعلومات والاتصالات.

ورغم أن المشرع الجزائري قد حدد مجموعة من الشروط الهامة، فإن النصوص القانونية لم تورد تفاصيل دقيقة بشأن المتطلبات الفنية والتقنية. على سبيل المثال، لم يحدد المشرع كيفية تقييم الخبرات أو تحديد المعايير التقنية التي يجب أن يتوفر عليها مقدمو خدمات التصديق الإلكتروني. هذه النقطة تثير تساؤلات حول كيفية تقييم هذه الشروط من الناحية الفنية. بالمقابل، تتيح تشريعات دول أخرى مثل فرنسا ومصر تفاصيل دقيقة فيما يتعلق بالمتطلبات التقنية. ففي فرنسا، يتم فرض استخدام تقنيات تشفير قوية لضمان حماية البيانات ومنع التلاعب أو التزوير، كما يتم التأكد من كفاءة الكوادر الفنية. أما في مصر، فتتضمن التشريعات تحديد شروط ضمان مالي لمقدمي الخدمة لتغطية الأضرار التي قد تنشأ نتيجة لأي إخلال بالالتزامات.

وفيما يخص إجراءات منح التراخيص في الجزائر، فقد اكتفى المشرع بتنظيم مرحلة ما بعد إصدار شهادة التأهيل، التي تُمنح لمدة سنة قابلة للتجديد. كما أوجب المشرع على مقدم الخدمة الحصول على الترخيص خلال 60 يومًا من استلام طلب الترخيص. ورغم ذلك، يلاحظ أن المشرع لم يتطرق بشكل كافٍ إلى تنظيم التفاصيل المتعلقة بالإجراءات التي تسبق إصدار شهادة التأهيل، وهو ما يترك بعض الغموض في هذه المرحلة. لذلك، من الأنسب أن يتدخل المشرع الجزائري بشكل أدق لتوضيح وتنظيم الإجراءات المتعلقة بالحصول على الترخيص قبل مرحلة إصدار شهادة التأهيل. هذا سيساهم في تقديم خدمات تصديق إلكتروني أكثر أمانًا وموثوقية، ويعزز الامتثال للمعايير الدولية.

بناءً على ما سبق، من الضروري أن يسعى المشرع الجزائري إلى مزيد من التفصيل والتوضيح في الشروط والمعايير التقنية المتعلقة بتقديم خدمات التصديق الإلكتروني، بما يضمن مستويات عالية من الأمان، ويعزز الثقة في هذا القطاع. كما يجب تنظيم الإجراءات القانونية بشكل أكثر وضوحًا لتجنب أي لبس، بما يتماشى مع المعايير العالمية.

ثالثا: التزامات مؤدي خدمات التصديق الالكتروني

تتعدد وتتنوع الالتزامات الملقاة على عاتق مقدمي خدمات التصديق الالكتروني، وهي كالتالي[94]:

1- الالتزام بتأدية خدمات التصديق الالكتروني وفقاً لسياسة التصديق المرخص له بها.

يفرض على مؤدي خدمات التصديق الالكتروني لغرض تأمين المعاملات الالكترونية وضمان تأدية الخدمات المرخص لهم بها وفقاً لسياسة التصديق الخاصة بهم والموافق عليها من قبل السلطة المختصة بذلك[95]

2- الالتزام بالتأكد من صحة البيانات المقدمة وبالحفاظ عليها

التي يتلقاها من الموقعين ، وذلك لأن عدم صحتها قد يلحق ضرراً بالأشخاص الذين يعتمدون على هذه الشهادات في التحقق من هوية الموقع وقدرته على ابرام المعاملات الالكترونية مما يرتب مسؤولية مقدمي خدمات التصديق الالكتروني والزامهم بجبر الضرر[96].

وقد اشترط المشرع الجزائري لتنفيذ هذا الالتزام على مؤدي خدمات التصديق الالكتروني عدم امكانه جمع البيانات الشخصية للمعني إلاّ بعد موافقته الصريحة، كما انه لا يمكنه أن يطلق يده في جمع البيانات الشخصية لصاحب التوقيع والشهادة، ولا يجمع منها إلاّ ما هو ضروري لمنح وحفظ شهادة التصديق الالكتروني ولا يمكنه استعمالها لأغراض أخرى خارج نشاط التصديق، كما ألزمه بالتحقق من التكامل والتطابق بين منظومة وبيانات إنشاء التوقيع الالكتروني مع منظومة وبيانات التحقق فيه[97].

3- الالتزام بإصدار أدوات انشاء وتثبيت التواقيع الالكترونية إلى كل من يطلب منهم هذه الخدمة، وذلك وفقاً للشروط والإجراءات والضوابط المحددة قانوناً

4- الالتزام بإصدار شهادات التصديق الالكتروني لمن يطلبها طوال مدة الترخيص وفقاً للمتطلبات الفنية والتقنية المشترطة فيها سلفاً في القوانين المنظمة لها[98]، على أن تترتب ضده المسؤولية القانونية في حالة ما إذا وجد أي إخلال بها[99]. كما ألزمته كذلك بضمان تحديث البيانات الواردة فيها كلما استجدت معلومات حديثة عن أصحابها، وذلك طيلة فترة سريانها، وتعليق العمل بها مؤقتاً أثناء مدة سريانها أو إلغائها بشكل نهائي[100]، كلما توافرت المبررات القانونية التي تقضي بذلك، وتبليغ التعليق أو الالغاء للمعني به ونشره للغير وفقاً لسياسة التصديق الالكتروني الموافق عليها.+

---

[94] - ينظر في ذلك لنصوص المواد ((41 إلى 50) من قانون التوقيع والتصديق الالكترونيين الجزائري.

[95] - ورد في نص المادة 41 من قانون التوقيع والتصديق الالكتروني رقم 15-04 التي نصت على أن:" يكلف مؤدي خدمات التصديق الالكتروني بتسجيل وإصدار ومنح وإلغاء ونشر وحفظ شهادات التصديق الالكتروني وفقاً لسياسة التصديق الالكتروني الخاصة به والتي وافقت عليها السلطة الاقتصادية للتصديق الإلكتروني".

[96] - أيمن مساعدة، التوقيع الرقمي وجهات التوثيق، مؤتمر القانون والحاسوب، 12 إلى 14 تموز 2004، جامعة اليرموك، كلية القانون، اربد، الاردن، ص 19.

[97]- ينظر لنصي المادتين (43 و44) من قانون التوقيع والتصديق الإلكترونيين رقم 15-04

[98]- يرجع لنصوص مواد الملحق I من التنظيم الاوروبي رقم 910-2014، المادة (15) من قانون التوقيع والتصديق الالكترونيين الجزائري رقم 15-04.

[99]- ينظر نص المادة 53 من قانون التوقيع والتصديق الالكتروني رقم 15-04.

[100] - ينظر المادتين (45 و46) من قانون التوقيع والتصديق الالكتروني الجزائري رقم 15-04.

5- الالتزام بحفظ مفاتيح التشفير الخاصة[101]، كأدوات فنية يحوزها الموقعين بصفة شخصية، وتستخدم لإنشاء التواقيع الالكترونية ونظراً لخطورتها لإمكانية استخدامها من الغير إذا ما وقعت في يده، فقد حرص التشريع الجزائري على اشتراط ضرورة أن تكون في حيازة الموقع نفسه وتحت سيطرته التامة حتى يحوز التوقيع الالكتروني المنشئ بها على الحجية القانونية في الاثبات[102].و تم الزام الموقع نفسه بالمحافظة على سرية العناصر السرية الخاصة به واتخاذ العناية الكافية والتدابير اللازمة لاجتناب استخدامها من الغير[103]. كما منع كذلك بصفة مطلقة على مقدم خدمات التصديق الالكتروني إمكانية حفظ أو نسخ بيانات إنشاء التوقيع الالكتروني بما فيها مفاتيح التشفير الخاصة بالأشخاص الذين منحت لهم شهادات التصديق الالكتروني الموصوفة[104].

6- **الالتزام بتقديم خدمة الختم الزمني الالكتروني "l'horodatage électronique "** الذي التنظيم الاوروبي رقم 910-2014 عرفه بموجب المادة (33/03) منه بأنه:" بيانات في شكل الكتروني ترتبط بيانات آخرى في شكل الكتروني في وقت معين لإقامة الدليل على أنّها وجدت في ذلك الوقت"، ومن ثمة فإنّه يمكن لمقدمي خدمات الثقة تقديم خدمة التحديد الدقيق لتاريخ وساعة انشاء وارسال واستلام أي بيانات الكترونية معينة، وخدمة كهذه تساهم إلى حد كبير في تأمين ودقة المعاملات الالكترونية، كما انّها ضرورية لبدء الآثار القانونية في بعض التصرفات القانونية.

7- الالتزام بالحفاظ على سرية البيانات التي يتلقاها من الموقعين أو بترخيص منهم[105]، بموجب المادة 42 من قانون التوقيع والتصديق الالكترونيين التي نصت على أنّه:" يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة"، وإن كان ينبغي على المشرع الجزائري في هذه المادة ان لا يكتفي فقط بالنص على الحفاظ على سرية البيانات المتعلقة بشهادات التصديق الالكتروني فقط، بل يجعل من هذا الالتزام يشمل جميع البيانات التي تكون متعلقة بأنشطتهم ومختلف خدماتهم المقدمة من طرفهم.

8- الالتزام بالشفافية وعدم التمييز وبالاستمرارية بتأدية الخدمات من خلال نص المادة 58 من قانون التوقيع والتصديق الالكترونيين التي نصت على أنّه:" يجب على مؤدي خدمات التصديق الالكتروني إعلام السلطة الاقتصادية للتصديق الالكتروني في الآجال المحددة في سياسة التصديق لهذه السلطة برغبته في وقف نشاطاته المتعلقة بتأدية خدمات التصديق الالكتروني أو بأي فعل قد يؤدي إلى ذلك، وفي هذه الحالة يلتزم مؤدي خدمات التصديق الالكتروني بأحكام سياسة التصديق

---

[101]- وقد عرّف المشرع الجزائري مفتاح التشفير الخاص بموجب المادة (8/2) من قانون التوقيع والتصديق الالكترونيين رقم 15-04 بأنّه:" عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع فقط، وتستخدم لإنشاء التوقيع الالكتروني، وترتبط بمفتاح التشفير العمومي"، وقد عرّفه المشرع المصري بتعريف مشابه لهذا التعريف غير أنّ اضاف إمكانية ان يتم الاحتفاظ به على بطاقة ذكية مؤمنة، يرجع لنص المادة (1/12) من اللائحة التنفيذية لقانون التوقيع الالكتروني المصري رقم 15 لعام 2004.

[102]- مثل ما ورد في المادة (07) من قانون التوقيع والتصديق الالكترونيين الجزائري.

[103] - وفي هذا قرّرت المادة (61/ 1 و2) من قانون التوقيع والتصديق الالكترونيين رقم 15-04 أنّه:" يعتبر صاحب شهادة التصديق الالكتروني فور التوقيع عليها المسؤول الوحيد عن سرية بيانات إنشاء التوقيع. وفي حالة الشك في الحفاظ على سرية بيانات إنشاء التوقيع أو في حالة ما إذا أصبحت هذه البيانات غير مطابقة للمعلومات المتضمنة في شهادة التصديق الالكتروني فإنه يجب على صاحب الشهادة أن يعمل على إلغائها من طرف مؤدي خدمات التصديق الإلكتروني".

[104] - وذلك بموجب المادة 48 من قانون التوقيع والتصديق الالكتروني رقم 15-04.

[105]- ينظر في ذلك لنصوص المواد (21) من قانون التوقيع الالكتروني المصري لعام 2004، (15) من القانون التونسي الخاص بالمبادلات و التجارية الإلكترونية عدد 83 لعام 2000، (25) من القانون المغربي رقم 05-53 الخاص بالتبادل الإلكتروني للمعطيات القانونية...

الالكتروني للسلطة الاقتصادية المتعلقة باستمرارية الخدمة ويترتب على وقف النشاط سحب الترخيص"[106].

كما ألزم المشرع الجزائري بشكل صريح كذلك مؤدي خدمات التصديق الالكتروني من خلال قانون التوقيع والتصديق الالكتروني رقم 15-04 بتقديم خدماته في إطار مبدئي الشفافية وعدم التمييز، وفي سبيل ذلك منعه من إمكانية رفضه لتقديم خدماته بدون سبب وجيه، ويعود السبب وراء ذلك في رغبة المشرع الجزائري في إقرار مبدأ عدم التمييز والمساواة فيما بين الموطنين المنتفعين وحمايتهم من تعسف مؤدي خدمات التصديق الالكتروني.

وقد نصت المادة 53 منه على مسؤولية مؤدي خدمات التصديق الالكتروني الذي سلم شهادة تصديق الكتروني موصوفة عن الضرر الذي يلحق بأي شخص طبيعي أو معنوي، اعتمد على شهادة التصديق الالكتروني هذه، وذلك فيما يخص: 1- صحة جميع المعلومات الواردة في شهادة التصديق الالكتروني الموصوفة في التاريخ الذي منحت فيه، ووجود جميع البيانات الواجب توافرها فيها. 2- التأكد عند منح شهادة التصديق الالكتروني الموصوفة أنّ الموقع الذي تّم تحديد هويته فيها يحوز كل بيانات إنشاء التوقيع الموافقة لبيانات التحقق من التوقيع المقدمة و /أو المحددة فيها. 3- التأكد من إمكانية استعمال بيانات إنشاء التوقيع والتحقق منه بصفة متكاملة".[107].

المطلب الثاني: الحفظ الإلكتروني كآلية لضمان سلامة الإثبات المدني الرقمي

يُعد التحول الرقمي من أبرز مظاهر العصر الحديث، حيث أصبحت تكنولوجيات الإعلام والاتصال ركيزة أساسية في تطوير أنظمة المعاملات المدنية والإدارية، الأمر الذي فرض إعادة النظر في آليات الإثبات التقليدية بما يواكب هذا التطور. وفي هذا السياق، برز **الحفظ الإلكتروني** كأحد أهم تطبيقات تكنولوجيا المعلومات، إذ أتاح إمكانيات متقدمة في تخزين الوثائق والمحررات الرقمية بطريقة تضمن سلامتها وحجيتها أمام الجهات القضائية. وتكمن أهمية الحفظ الإلكتروني في كونه لا يقتصر فقط على تأمين البيانات، بل يُسهم أيضًا في إرساء الثقة في البيئة الرقمية، ويضمن حماية حقوق الأفراد والمؤسسات، من خلال حفظ الأدلة الإلكترونية بشكل يضمن ثباتها وسهولة الرجوع إليها دون تغيير أو تلاعب. ومن هنا، فإن الحفظ الإلكتروني يُعد آلية حديثة لتعزيز أمن المعلومات القانونية وضمان سلامة أدلة الإثبات المدني في إطار البيئة الرقمية المدعومة بتكنولوجيات الإعلام والاتصال.

من أجل استيعاب الدور الحيوي الذي يضطلع به **الحفظ الإلكتروني** في مجال الإثبات المدني الإلكتروني، لا بد من تحليل عناصره القانونية والتقنية، في ارتباط وثيق بتطور تكنولوجيات الإعلام والاتصال، وذلك على النحو الآتي:

الفرع **الأول: مفهوم الحفظ الالكتروني**

---

[106]- كما نصت كذلك المادة (59) من ذات القانون على أنّه:" يجب على مؤدي خدمات التصديق الالكتروني الذي يوقف نشاطه لأسباب خارجة عن ارادته أن يعلم السلطة الاقتصادية بذلك فوراً وتقوم هذه الأخيرة بإلغاء شهادته للتصديق الالكتروني الموصوفة بعد تقدير الأسباب المقدمة".

[107] - كما نصت المادة 54 من ذات القانون على مسؤولية مؤدي خدمات التصديق الالكتروني الذي سلم شهادة التصديق الالكتروني الموصوفة عن الضرر الناتج عن عدم إلغاء شهادة التصديق الالكتروني، والذي يلحق بأي شخص طبيعي أو معنوي اعتمد عليها

يُعد الحفظ الإلكتروني من المرتكزات القانونية الأساسية التي تبنتها التشريعات المقارنة، سواء على المستوى الدولي أو الإقليمي أو الوطني، كشرط جوهري لاكتساب الكتابة الإلكترونية حجيتها القانونية أمام القضاء. فقد أجمعت مختلف الأنظمة القانونية الحديثة على أن ضمان سلامة الدليل الكتابي الإلكتروني لا يتحقق إلا من خلال حفظه في ظروف تقنية وأمنية تمنع تعرضه لأي تغيير أو تحريف. وفي السياق الجزائري، كرّس المشرّع هذا المبدأ من خلال **المادة 323 مكرر 1 من القانون المدني الجزائري**، والتي تنص صراحة على أن" :الكتابة الإلكترونية تتمتع بنفس الحجية التي تتمتع بها الكتابة على الدعامة الورقية، شريطة أن تتيح هذه الكتابة التعرف على الشخص الذي صدرت عنه، وأن يتم حفظها في ظروف تضمن سلامتها ".ويعكس هذا النص ارتباط قوة الإثبات المدني الإلكتروني بتحقق شرطين متكاملين: أولًا، تحديد هوية الشخص الذي صدرت عنه الكتابة؛ وثانيًا، حفظها في بيئة تكنولوجية مؤمنة تضمن سلامة البيانات وعدم قابليتها للتلاعب. ويرجع هذا الاشتراط إلى الطبيعة اللامادية للوسائط الرقمية التي تُثبت عليها الكتابة أو التوقيع الإلكتروني، والتي تُمكن من فصلها أو التعديل عليها بطرق يصعب كشفها دون آليات تقنية متقدمة، مما يبرز الحاجة إلى اعتماد نظام موثوق للحفظ الإلكتروني، يُسهم في استقرار المعاملات الإلكترونية ويُعزز الثقة القانونية في محتواها.

التشريع الجزائري كرّس مبدأ الحفظ الإلكتروني بموجب المرسوم التنفيذي رقم 16-142[108] الصادر بتاريخ 5 مايو 2016، الذي حدد كيفية حفظ الوثائق الموقعة إلكترونيًا. حيث تناول المرسوم في مادته الثانية بعض المصطلحات والعبارات المستخدمة فيه، ومن بينها تعريف الحفظ الذي عرّفه المشرع الجزائري بأنه "مجموعة من التدابير التقنية التي تسمح بتخزين الوثيقة الموقعة إلكترونيًا في دعامة الحفظ". بذلك، قدّم المشرع الجزائري تعريفًا تقنيًا للحفظ يعتمد بشكل رئيسي على التقنيات الفنية المستخدمة في تأمين الوثائق الإلكترونية. وبذلك يتكامل هذا التعريف مع ما تم الإشارة إليه في القانون المدني الجزائري، الذي يشترط حفظ الكتابة الإلكترونية في ظروف تضمن سلامتها وتمنع تعرضها للتعديل أو التحريف، مما يعزز من قوة الإثبات القانوني لها في المعاملات الإلكترونية.

ويرى بعض الفقهاء أن الحفظ الإلكتروني يُقصد به تخزين بيانات الكتابة والتوقيع الإلكترونيين على دعامة إلكترونية ثابتة لا يمكن تعديل محتواها إلا من قبل صاحبها، ولا يمكن للغير الوصول إليها إلا بعلمه وموافقته. ويتضمن هذا المفهوم شقين أساسيين: أولهما، تحميل البيانات على دعامة إلكترونية مناسبة وآمنة، غير قابلة للاستنساخ، ومحمية بكلمة مرور أو وسائل تقنية تحقق السرية والحماية. أما الشق الثاني، فيتمثل في حفظ هذه الدعامة في مكان آمن وبعيد عن متناول الغير، بما يضمن بقاء البيانات في مأمن من أي اطلاع أو تعديل غير مشروع[109]

في العديد من المجالات التقنية، قد شاع استخدام مصطلح آخر يعبر عن الحفظ الإلكتروني وهو "الأرشفة الإلكترونية". يشير هذا المفهوم إلى مجموعة من الإجراءات والأدوات التي تستخدم لتخزين وتنظيم المحتويات الإلكترونية على وسائط آمنة، مما يضمن سهولة استرجاعها واستخدامها عند الحاجة، سواء لأغراض قانونية أو إدارية. ورغم تشابه الحفظ الإلكتروني مع

---

[108] - المرسوم التنفيذي رقم 16-142 الصادر بتاريخ 05 ماي 2016 المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونياً، منشور بالجريدة الرسمية عدد 28، بتاريخ 08 ماي 2016، ص 12 و13.

[109] - أيمن سعد سليم، التوقيع الالكتروني، دار النهضة العربية، القاهرة، 2004، ص 55. زيد حمزة مقدم، وسائل وضمانات التوثيق الالكتروني، مقال بمجلة جامعة بحري للآداب والعلوم الانسانية، السودان، السنة الثالثة، العدد السادس، ديسمبر 2014، ص 173.

الأرشفة الإلكترونية، إلا أن هناك فرقاً بينهما. فالحفظ الإلكتروني يركز على ضمان سلامة البيانات وحمايتها من التعديل أو التحريف أثناء تخزينها، بينما الأرشفة الإلكترونية تشمل تنظيم الوثائق بشكل يسمح بالوصول إليها واستخدامها بفعالية في المستقبل. يمكن القول أن الحفظ جزء من الأرشفة لكنه يركز على الأمان، بينما الأرشفة تهتم بالتنظيم والاسترجاع.

ونتيجة لكل ما سبق يمكن القول بأنّ الحفظ الإلكتروني لأدلة الإثبات المدنية هو العملية القانونية والتقنية التي تهدف إلى تأمين سلامة الكتابة والتوقيع الإلكترونيين من أي تغيير أو تحريف قد يطرأ عليهما، وذلك عبر جميع مراحل حياتهما، بدءًا من لحظة إنشائهما، مرورًا بعمليات نقلهما وإرسالهما والتحقق منهما، وانتهاءً بالتصديق عليهما، مع ضمان إمكانية الرجوع إليهما لاحقًا بنفس الصورة التقنية التي كانا عليها، وعلى مدى زمني طويل يمتد طيلة فترة تقادم الدليل القانوني. ويتم هذا الحفظ وفق معايير تشريعية وتقنية دقيقة، تفرض على مقدمي خدمات التصديق والحفظ الإلكتروني اعتماد أنظمة موثوقة تضمن السرية، والأمان، واستمرارية صلاحية المفاتيح وشهادات التصديق، بما يُمكّن من الاحتجاج بالكتابة الإلكترونية والتوقيع الإلكتروني أمام القضاء بثقة واطمئنان قانوني.

الفرع الثاني: التنظيم التشريعي لآلية الحفظ الالكتروني

تمثل آلية الحفظ الإلكتروني أحد الركائز الأساسية التي تضمن حماية المستندات الإلكترونية وتوثيقها على المستويات الدولية والإقليمية والوطنية. وقد تم اتخاذ عدة مبادرات تشريعية من أجل تنظيم هذه الآلية، مع التأكيد على ضرورة توافر شروط قانونية محددة لضمان اعتبار هذه الوثائق كأدلة قانونية مقبولة في المحكمة.

وعلى الصعيد الدولي، حرص قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لعام 1996 على تحديد شروط الاحتفاظ برسائل البيانات، لكي تكون مقبولة للإثبات القضائي. في هذا السياق،نص هذا القانون في المادة 10 على أنه يجب أن يتم الاحتفاظ برسائل البيانات بطريقة تضمن الاطلاع عليها واستخدامها لاحقًا، مع التأكيد على ضرورة الحفاظ على محتوى الرسالة بالشكل الذي تم إنشاؤه أو إرساله أو استلامه، إضافة إلى إمكانية استبيان منشأ الرسالة ووجهتها وتاريخ ووقت إرسالها واستلامها.

من جانب آخر، المشرع الأوروبي تناول في تنظيمه رقم 2014/910 الصادر عن البرلمان الأوروبي في 23 يوليو 2014، مسألة الحفظ الإلكتروني للتوقيعات الإلكترونية والأختام والشهادات المرتبطة بها. وفقًا للمادة 16، تتضمن "خدمة الثقة" إنشاء وتحقيق التوقيعات الإلكترونية والأختام الإلكترونية بالإضافة إلى حفظ هذه العناصر بطرق موثوقة. كما أشار التنظيم الأوروبي إلى ضرورة أن تتم خدمة الحفظ من قبل مقدمي خدمات موثوقة، والذين يجب أن يلتزموا بإجراءات تكنولوجية تسمح بتمديد موثوقية التوقيعات بعد التحقق الأولي من صحتها.

اويتبين من خلال النصوص السابقة أن الحفظ الإلكتروني، باعتباره جزءًا من خدمات الثقة، يعتمد على تقنيات تكنولوجية معقدة لضمان سلامة الوثائق وحمايتها من التلاعب. على الصعيد الأوروبي، تم تحديد معايير خاصة تتعلق بخدمات الحفظ الموصوف للتوقيعات الإلكترونية، حيث يشترط أن يقوم بها مقدم خدمة موثوق وفقًا لإجراءات تكنولوجية معتمدة، مما يعزز من مصداقية التوقيعات الإلكترونية ويضمن حفظها لفترات طويلة بشكل موثوق.

وعلى الصعيد الوطني فقد حدد المشرع الجزائري[110] في القانون التوقيع والتصديق الإلكتروني رقم 15-04 كيفية حفظ الوثائق الموقعة إلكترونيًا، حيث اشترط أن يتم حفظها في شكلها الأصلي، مع توجيه التنظيم لتحديد التفاصيل المتعلقة بكيفية الحفظ. بناءً على ذلك، صدر المرسوم التنفيذي رقم 16-142 بتاريخ 5 مايو 2016، الذي يحدد آلية حفظ الوثائق الموقعة إلكترونيًا. وتضمن المرسوم 10 مواد، التي تحدد الشروط الواجب توافرها لحفظ ونقل الوثائق الموقعة إلكترونيًا، كما توضح الأشخاص الملزمين بالامتثال لهذه الشروط، بالإضافة إلى تحديد شكل دعامة الحفظ وفترة الحفظ.

وفي المادة 02 من ذات المرسوم، تم تعريف بعض المصطلحات المستخدمة فيه، حيث تم تعريف الوثيقة الموقعة إلكترونيًا بأنها "وثيقة إلكترونية مرفقة أو متصلة منطقياً بتوقيع إلكتروني". كما تم تعريف الحفظ بأنه "مجموعة من التدابير التقنية التي تتيح تخزين الوثيقة الموقعة إلكترونيًا في دعامة الحفظ". أما باقي المواد، فقد تناولت الشروط القانونية الواجب توافرها في حفظ الوثائق الموقعة إلكترونيًا، وحددت التزامات مقدمي خدمات الحفظ الإلكتروني والعملاء المعنيين وسيتم معالجتها فيمايلي من الدراسة..

الفرع الثالث: الشروط المطلوبة للحفظ الالكتروني

يتضح من استعراض مختلف النصوص القانونية الدولية والإقليمية والوطنية المتعلقة بالحفظ الإلكتروني للكتابة والتوقيع الإلكتروني، وجود تفاوت في كيفية تنظيم الشروط القانونية لضمان سلامة هذه العناصر والاعتداد بها في الإثبات. ويبرز هذا التباين بين ما جاء في قانون الأونسيترال النموذجي للتجارة الإلكترونية لعام 1996، وما نص عليه التنظيم الأوروبي رقم 910-2014.

ففي المادة 10 من قانون الأونسيترال، اعتُبر الاحتفاظ برسائل البيانات ملبياً لمتطلبات القانون إذا توفرت الشروط التالية: أ –إمكانية الاطلاع على المعلومات عند الحاجة، ب –حفظ الرسالة بالشكل الأصلي أو بما يعكسها بدقة، ج –الاحتفاظ بمعلومات تحدد مصدر الرسالة، وجهة إرسالها، وتاريخ ووقت إرسالها واستلامها.

أما المادة 34 من التنظيم الأوروبي رقم 910-2014، فقد نصّت على أن خدمة الحفظ الموصوف للتوقيعات الإلكترونية الموصوفة لا تُقدَّم إلا من قبل مقدّم خدمات موصوف مؤهل وخاضع لإشراف الجهة المختصة، ويشترط أن يستخدم هذا المقدم إجراءات وتكنولوجيات تضمن تمديد موثوقية التوقيع إلى ما بعد انتهاء صلاحيته التقنية. كما خوّلت اللجنة الأوروبية صلاحية تحديد المعايير المرجعية الواجب احترامها.

بذلك، يظهر أن القانون الأوروبي اعتمد نهجًا أكثر دقة وتنظيماً من خلال اشتراط التأهيل والرقابة، إضافة إلى توحيد المعايير التقنية، على خلاف ما ركز عليه قانون الأونسيترال من شروط تتعلق بالشكل والمحتوى فقط.

[110] - المادة 04 من قانون التوقيع والتصديق الإلكتروني رقم 15-04 .

وفي التشريع الجزائري، نصت المادة 04 من قانون التوقيع والتصديق الإلكترونيين رقم 15-04 على أنه "يجب حفظ الوثيقة الموقعة إلكترونيًا في شكلها الأصلي، ويتم تحديد الكيفيات المتعلقة بحفظها عن طريق التنظيم". بناءً على هذا النص، تم إصدار المرسوم التنفيذي رقم 16-142 بتاريخ 5مايو 2016، الذي حدد كيفية وشروط حفظ الوثيقة الموقعة إلكترونيًا، بما في ذلك شكل دعامة حفظها ومدة حفظها. وهذه الشروط كالتالي:

1- الشروط المتعلقة بالبيانات محل الحفظ الالكتروني

حدد المشرع الجزائري في المادة 03 من المرسوم التنفيذي رقم 16-142 المتعلق بكيفيات حفظ الوثيقة الموقعة إلكترونياً أنه يجب ضمان استرجاع الوثيقة في شكلها الأصلي والتحقق من توقيعها الإلكتروني. كما بينت المادة 04 من نفس المرسوم البيانات الأساسية التي يجب أن يتضمنها الحفظ الإلكتروني للوثائق الموقعة إلكترونياً، وهي: الوثيقة الإلكترونية وتوقيعها الإلكتروني، شهادة التصديق الإلكتروني للموقع، قائمة الشهادات الإلكترونية الوسيطة حتى الوصول إلى السلطة الوطنية للتصديق الإلكتروني، قوائم الشهادات الملغاة أو نتائج التحقق من حالة الشهادات الإلكترونية الوسيطة، وتاريخ توقيع الوثيقة عند الاقتضاء. هذه البيانات تضمن سلامة الوثيقة وتحافظ على موثوقيتها في أي وقت يتم استرجاعها أو التحقق منها.

2- الشروط المتعلقة بدعامة الحفظ الالكتروني

عرّفت الفقرة الثالثة من المادة 2 من المرسوم التنفيذي الجزائري رقم 16-142 دعامة الحفظ الإلكتروني بأنها: "أي وسيلة مادية أيّاً كان شكلها أو خصائصها المادية، تسمح باستلام وحفظ واسترجاع الوثيقة الموقعة إلكترونياً". وبذلك ترك المشرع الجزائري المجال مفتوحاً لاستخدام أي نوع من الوسائط المادية، كالأقراص الممغنطة، أو الضوئية، أو المدمجة، أو الذواكر الإلكترونية، شرط أن تكون قادرة على أداء مهام الاستلام والحفظ والاسترجاع بكفاءة.

وقد أوجبت المادة 6 (فقرتان 1 و2 (من نفس المرسوم توافر شرطين أساسين في دعامة الحفظ. أولاً، يجب أن تُمكّن من استرجاع الوثيقة والاطلاع الكامل على محتواها في أي وقت عبر الوسائل التقنية المناسبة. وثانياً، يتعين على المسؤول عن الحفظ استخدام هذه الدعامة وفق شروط تضمن سلامتها وحسن سيرها، لضمان حماية محتواها من التلف أو التعديل غير المقصود.

وفي حال تم نقل الوثيقة الموقعة إلكترونياً من دعامة حفظ إلى أخرى، نصّت المادة 7 على وجوب أن يشمل النقل جميع العناصر التي تحتويها الوثيقة، وفق ما هو محدد في المادة 4 من نفس المرسوم. كما اشترطت التحقق من التوقيع الإلكتروني بعد عملية النقل لضمان الحفاظ على صحتها القانونية.أما المادة 8، فقد شددت على ضرورة الحفاظ على الشكل الأصلي للوثيقة، مؤكدة أنّ كل عملية تُجرى على الوثيقة لأسباب تتعلق بالفعالية أو الأمن يجب أن تتيح إمكانية استرجاعها دون أي تعديل أو تغيير في محتواها أو شكلها.

3- الشروط المتعلقة بمدة الحفظ الالكتروني

فيما يخص مدة حفظ الكتابات الموقعة إلكترونيًا، تختلف النصوص القانونية حسب نوع المعاملة. ففي المعاملات المدنية البحتة، لا يُلزم القانون بحفظ الوثائق الإلكترونية لمدة محددة، إلا إذا ورد نص خاص بذلك في القانون المدني أو قانون الإثبات، وتكون مدة الحفظ على الأقل

مساوية لمدة تقادم الحق المثبت فيها. وتُعد مدد التقادم هي الحد الأدنى للحفظ، مع إمكانية الإبقاء على الوثائق لمدد أطول بفضل الوسائط الإلكترونية المتطورة القادرة على حفظ البيانات لفترات طويلة دون تلف. وتشكل أحكام القانون المدني المرجع العام لمدد تقادم العقود، ما لم تُقيَّد بنصوص خاصة في قوانين الإثبات الإلكتروني.

أما في المعاملات التجارية، فغالبًا ما يفرض القانون التجاري مددًا محددة لحفظ الوثائق، بغض النظر عن مدد التقادم. وقد تبنى المشرع الجزائري هذا التوجه، حيث نصّت المادة 12 من القانون التجاري على ضرورة حفظ الدفاتر والمستندات (المواد 9 و10) والمراسلات لمدة 10 سنوات .وبالنسبة للوثائق الإلكترونية، تنص المادة 09 من المرسوم التنفيذي رقم 16-142 لسنة 2016 على حفظ الوثيقة خلال مدة منفعتها، ما يفتح المجال لتقدير مدة الحفظ بحسب طبيعة الوثيقة والنصوص التنظيمية أو اتفاق الأطراف. ومن أبرز الأمثلة على ذلك، القرار رقم 19 الصادر في 31 ماي 2017 عن سلطة الضبط للبريد والمواصلات، الذي ألزم بحفظ العقود والوثائق الإلكترونية لتحديد هوية الزبائن لمدة 15سنة من تاريخ فسخ الاشتراك، وذلك استنادًا إلى القرار رقم 71 الصادر بتاريخ 28 أكتوبر 2015.

الفرع الرابع: النظام القانوني لمؤدي خدمات الحفظ الالكتروني

يشمل النظام القانوني للقائم على تقديم خدمات الحفظ الإلكتروني تحديد دور هذه الجهات، وتنظيم التزاماتها ومسؤولياتها، سواء من الناحية التقنية أو القانونية. كما يعكس هذا النظام المعايير التي يجب أن تلتزم بها هذه الجهات لتوفير بيئة إلكترونية موثوقة وآمنة، بما يساهم في بناء الثقة في المعاملات الرقمية.

أولا-المسئول عن تقديم خدمة حفظ التوقيع والكتابة الإلكترونية

الأصل في مسؤولية حفظ التوقيعات والكتابات الإلكترونية يقع على أصحابها، حيث أن حماية هذه الوثائق من العبث أو الضياع تعتبر مصلحة شخصية لهم. ومع ذلك، تتطلب عملية الحفظ الإلكتروني مهارات تقنية عالية وكفاءة خاصة، مما يستدعي تدخل طرف ثالث موثوق فيه يمتلك هذه المؤهلات لضمان سلامة الوثائق الموقعة إلكترونيًا مقابل أجر محدد.

وعلى الرغم من أهمية دور الطرف الثالث في تقديم خدمة الحفظ الإلكتروني، لم يتم تحديد المسؤول بشكل واضح في العديد من التشريعات الوطنية والدولية، بما في ذلك قانون الأونسترال النموذجي بشأن التجارة الإلكترونية لعام 1996. في المادة 03/10 من هذا القانون، تم الإشارة إلى "الشخص الآخر" القادر على الوفاء بمتطلبات الحفظ، دون تحديد دقيق لمن هو هذا الطرف.

في التشريع الجزائري، نصت المادة 05 من المرسوم التنفيذي رقم 16-142 الصادر في 05 مايو 2016 على أن "كل شخص طبيعي أو معنوي موقّع أو مستلم لوثيقة موقعة إلكترونيًا يجب أن يضمن حفظها بنفسه أو عبر طرف ثالث." ومع ذلك، لم يتم تحديد الطرف الثالث المسؤول عن خدمة الحفظ الإلكتروني بشكل دقيق، مما يثير تساؤلات حول ما إذا كان هو نفس الطرف الذي يقدم خدمات التصديق الإلكتروني وغيرها من خدمات الثقة الإلكترونية، وما إذا كان يجب أن يخضع لنفس النظام القانوني من حيث الترخيص والشروط والواجبات.

في المقابل، قدم التنظيم الأوروبي [111]رقم 910-2014 الصادر في 23 يوليو 2014 تنظيمًا أكثر وضوحًا، حيث قام بتكليف مهمة حفظ التوقيعات والأختام الإلكترونية إلى جهة مسؤولة عن تقديم خدمات الثقة الإلكترونية الأخرى. عرف التنظيم الأوروبي "مقدم خدمات الثقة " بأنه "شخص طبيعي أو معنوي يقدم خدمة واحدة أو أكثر من خدمات الثقة" ومنها حفظ التوقيعات الإلكترونية والأختام الإلكترونية، كما نصت الفقرة (ج) على أن "خدمة الثقة تشمل حفظ التوقيعات الإلكترونية والأختام الإلكترونية أو الشهادات المتعلقة بها".

ثانيا- التزامات مؤدي خدمات الحفظ الالكتروني

في البداية، يجب الإشارة إلى أن الإطار القانوني المنظم لالتزامات مقدمي خدمات الحفظ الإلكتروني للكتابة والتوقيعات الإلكترونية لا يزال بحاجة إلى تحديد دقيق وواضح. فقد تناولت بعض التشريعات، بما في ذلك النصوص الجزائرية الواردة في المرسوم التنفيذي رقم 16-142، تنظيم الشروط القانونية المطلوبة لتوفير خدمة الحفظ الإلكتروني وضمان الاعتراف بها في المحاكم. ومع ذلك، تفتقر هذه التشريعات إلى نصوص صريحة تحدد التزامات الأطراف في عقود الحفظ الإلكتروني، وخاصةً التزامات مقدمي خدمات الحفظ. وقد يعود ذلك إلى رغبة المشرع في منح الأطراف حرية تحديد التزاماتهم وفقًا لمبدأ "العقود شريعة المتعاقدين"، مما يسمح لهم باتفاقات مرنة تتناسب مع متطلباتهم.

من ناحية أخرى، إذا اعتبرنا أن مقدمي خدمات الحفظ الإلكتروني هم نفسهم من يتولون تقديم خدمات التصديق الإلكتروني، فإن ذلك قد يتيح الرجوع إلى التشريعات التي وضحت الالتزامات المتعلقة بتقديم خدمات التصديق الإلكتروني. العديد من هذه التشريعات، بما في ذلك القانون الجزائري بشأن التوقيع والتصديق الإلكتروني، قد حددت بشكل دقيق واجبات مقدمي خدمات التصديق الإلكتروني. ومع ذلك، لا يمكن تطبيق هذه الالتزامات على مقدمي خدمات الحفظ الإلكتروني بشكل مباشر، لأن القوانين المتعلقة بخدمة التصديق الإلكتروني تركز غالبًا على شهادة التصديق نفسها وليس على خدمة الحفظ الإلكتروني أو إثباته.

لذلك، من الأنسب أن يقوم المشرع بإصدار نصوص قانونية محددة تنظم التزامات مقدمي خدمات الحفظ الإلكتروني، وتحدد المسؤولية القانونية في حالة الإخلال بتلك الالتزامات.

بناءً على النصوص القانونية المتوفرة التي تتعلق بشروط الحفظ الإلكتروني للكتابة والتوقيعات الإلكترونية، بالإضافة إلى النصوص التي تحدد التزامات مقدمي خدمات التصديق الإلكتروني، يمكن تلخيص أبرز الالتزامات التي تقع على عاتق مقدمي خدمات الحفظ الإلكتروني في النقاط التالية:

1- الالتزام بتأدية خدمات الحفظ الالكتروني للبيانات الالكترونية وفق الشروط المحددة قانوناً

يتعين على مقدم خدمة الحفظ الإلكتروني الالتزام بتخزين البيانات الإلكترونية وفقًا للمعايير القانونية المعتمدة، بحيث يتم الاحتفاظ بالمعلومات في شكلها الأصلي كما تم إنشاؤها أو إرسالها أو

[111] - المادة 16/03 من التنظيم الاوروبي.

استلامها، دون أي تعديل على محتوياتها. كما يجب أن تظل هذه المعلومات قابلة للاستخدام والرجوع إليها بسهولة، وتكون مفهومة وقابلة للقراءة من قبل أي شخص مخول له الوصول إليها.

ويتعين أيضًا على مقدم الخدمة إعداد سجل يتضمن المعلومات المتعلقة بالكتابة الإلكترونية وتوقيعها، بما في ذلك هوية الأطراف المعنية وتاريخ تخزين المعلومات. كما يجب أن يشمل السجل بيانات حول شهادات التصديق الإلكتروني، بما في ذلك الشهادات الوسيطة والملغاة، ونتائج التحقق من حالتها حتى الوصول إلى الجهة المختصة بالتصديق الإلكتروني.

علاوة على ذلك، يتعين عليه اختيار وسائل الحفظ الإلكترونية التي تفي بالمعايير القانونية وتتيح استرجاع المحتوى بشكل سليم في أي وقت عند الحاجة، مع ضمان الحفاظ على سلامة البيانات. كما يتوجب عليه الحفاظ على المعلومات طوال المدة المحددة قانونيًا أو وفقًا لما يتم الاتفاق عليه بين أطراف عقد الحفظ الإلكتروني، في حال غياب نص قانوني يلزم بمدة معينة للحفظ. في حالة إنهاء العقد، يلتزم بعدم إرسال المحفوظات إلا للأطراف المحددة في العقد، ما لم ينص القانون على [112]استثناءات.

2- الالتزام بتحديد وقت وتاريخ إنشاء البيانات محل الحفظ

يجب على مقدم خدمة الحفظ الإلكتروني تحديد وقت وتاريخ إنشاء وإرسال الكتابة والتوقيع الإلكترونيين، وهو ما يُعرف بالبصمة الزمنية الإلكترونية، لضمان حجية الكتابة الإلكترونية في المعاملات القانونية. وقد نص المشرع الجزائري في المادة 323 مكرر من القانون المدني على ضرورة ضمان سلامة الكتابة الإلكترونية مع التحقق من هوية من أصدرها، كما أوجب في المادة 04 من المرسوم التنفيذي رقم 16-142 تضمين تاريخ توقيع الوثيقة عند الحفظ، لضمان صحة البيانات وحمايتها من أي تعديل.

4- الالتزام بالحفاظ على سرية وسلامة البيانات المحفوظة

تفرض العديد من تشريعات التصديق الإلكتروني، بما في ذلك التشريع الجزائري وفقاً للمادة 42 من قانون التوقيع والتصديق الإلكترونيين، على مقدمي خدمات التصديق الحفاظ على سرية البيانات المتعلقة بشهادات التصديق الممنوحة. ومع ذلك، يُستحسن أن يشمل هذا الالتزام جميع البيانات المتعلقة بأنشطة مقدمي الخدمات، بما في ذلك خدمات الحفظ الإلكتروني والشهادات المرتبطة بها، مع النص على إمكانية الإعفاء من السرية في حالات معينة مثل الامتثال للقانون أو بناءً على طلب السلطات القضائية. بالإضافة إلى ذلك، يجب على مقدمي خدمات الحفظ الإلكتروني ضمان حفظ الكتابة والتوقيع الإلكتروني في ظروف آمنة تمنع أي تعديل، وتقديم النصح لعملائهم بشأن تقنيات الحفظ المناسبة وإعلامهم بأي تغييرات تقنية قد تؤثر على الحفظ الإلكتروني.

ويتحمّل مقدمو خدمات الحفظ الإلكتروني مسؤولية مدنية في حال إخلالهم بالالتزامات القانونية أو الفنية المرتبطة بحماية البيانات وسلامتها. وتتجلى هذه المسؤولية عندما يُلحق الإخلال ضررًا بالمستفيدين من الخدمة، حيث يتم تحديد طبيعة المسؤولية وفقًا لطبيعة العلاقة بين الأطراف. فإذا كانت العلاقة تعاقدية، فإن المسؤولية تكون عقدية ويحق للمتضرر المطالبة

[112] - ينظر في ذلك نص المواد 03 و04 و06 من المرسوم التنفيذي رقم 16-142 المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونياً.

بالتعويض وفقًا لأحكام العقد. أما في حال غياب العلاقة التعاقدية، فتخضع المسؤولية للأحكام العامة للمسؤولية التقصيرية، ويُشترط حينها إثبات الخطأ والضرر وعلاقة السببية وفقًا للقانون المدني الجزائري.

ورغم الأهمية المتزايدة لخدمات الحفظ الإلكتروني في العصر الرقمي، لا تزال التشريعات الجزائرية، على غرار العديد من الأنظمة القانونية المقارنة، تفتقر إلى نصوص قانونية خاصة تنظم المسؤولية المترتبة عن هذه الخدمات. وهو ما يدفع إلى الاعتماد على القواعد العامة للمسؤولية المدنية، على عكس ما هو معمول به في مجال خدمات التصديق الإلكتروني التي خُصّت بتنظيم قانوني مفصل يضع قرائن قانونية لصالح المتضرر. ويُبرز هذا الفراغ التشريعي الحاجة الماسّة إلى تدخل المشرّع الجزائري لإقرار إطار قانوني خاص بمسؤولية مقدمي خدمات الحفظ الإلكتروني، بما يضمن وضوحًا قانونيًا وحماية فعالة لحقوق الأفراد والمؤسسات في البيئة الرقمية.

الفصل الرابع: تكنولوجيات الإعلام والاتصال والجريمة الإلكترونية

تشكل تكنولوجيا الإعلام والاتصال سيفًا ذا حدين في عصرنا الحالي، حيث باتت تمثل أداة فعالة في تسهيل ارتكاب الجرائم كما أنها تقدم في الوقت نفسه الوسائل لمكافحتها. من جهة، تستخدم

الجريمة الإلكترونية وسائل التكنولوجيا الحديثة لارتكاب جرائم معقدة ومتنوعة مثل الاحتيال، الاختراق، والابتزاز، التي تستفيد من الطبيعة اللامحدودة والسرية التي توفرها الإنترنت والشبكات الرقمية. من جهة أخرى، توفر التكنولوجيا نفسها أدوات قوية للسلطات القانونية في مواجهة هذه الأنواع من الجرائم، مثل الأدلة الرقمية، تقنيات المراقبة، والذكاء الاصطناعي، التي تسهم في تحليل البيانات وتقديم الأدلة اللازمة للإدانة.

وبينما تسهم التكنولوجيا في تسهيل ارتكاب الجرائم الإلكترونية، تفتح أيضًا أمام الدول والمجتمعات فرصة لتطوير أدوات وتقنيات لمكافحة هذه الجرائم. إلا أن هذه المواجهة لا تخلو من تحديات قانونية وأخلاقية تتطلب توازنًا دقيقًا بين توفير الأمن وحماية الحقوق الفردية، مما يجعل التعامل مع هذه الظاهرة مسألة معقدة تتطلب تحديثًا مستمرًا للتشريعات والأطر القانونية لمواكبة التطور السريع في المجال التكنولوجي.

وتتناول الدراسة ضمن المبحثين المواليين: موضوع الجريمة الإلكترونية في سياق التطور التكنولوجي، حيث سنسلط الضوء على المفاهيم الأساسية المرتبطة بهذه الجرائم، ونوضح خصائصها وكيفية تمييزها عن الجرائم التقليدية. كما سنتناول تصنيف الجرائم الإلكترونية ودور الإنترنت في تسهيل تنفيذها. علاوة على ذلك، سيتم استعراض السياسات الجنائية المعاصرة لمكافحة هذه الجرائم، سواء على المستوى الوطني أو الدولي. في المقابل، سنناقش كيفية استخدام التكنولوجيا كأداة لمكافحة الجريمة، بما في ذلك استخدام الأدلة الرقمية والذكاء الاصطناعي في التحقيقات، إضافة إلى استعراض التحديات القانونية والأخلاقية التي ترافق توظيف التكنولوجيا في مكافحة الجريمة الإلكترونية وحماية الحقوق الفردية.

المبحث الأول: الجريمة الإلكترونية في ظل التطور التكنولوجي (التكنولوجيا كوسيلة لارتكاب الجريمة)

مع التطور المتسارع في تكنولوجيات الإعلام والاتصال، أصبحت هذه الوسائل لا تُستخدم فقط في تسهيل الحياة اليومية، بل استُغلت أيضًا كأدوات لارتكاب جرائم إلكترونية متنوعة .فقد أتاح الانتشار الواسع للإنترنت والحواسيب والهواتف الذكية للمجرمين تنفيذ أفعال غير مشروعة مثل الاحتيال الإلكتروني، والقرصنة، وانتهاك الخصوصية، دون الحاجة إلى التواجد المادي في موقع الجريمة .وقد أدرك المشرّع الجزائري هذه التحديات، فسعى إلى وضع إطار قانوني لمكافحة هذه الجرائم، من خلال تعديل قانون العقوبات وسنّ قوانين خاصة تتعلق بتكنولوجيات الإعلام والاتصال .يهدف هذا المبحث إلى دراسة مفهوم الجريمة الإلكترونية وخصائصها، بالإضافة إلى استعراض الإطار القانوني الجزائري المعتمد لمكافحتها.

المطلب الأول: مفهوم الجريمة الالكترونية

تُعدّ الجرائم الإلكترونية من أبرز التحديات القانونية التي فرضها التطور التكنولوجي في العصر الرقمي .وقد استدعى هذا الواقع من المشرّع الجزائري وضع إطار قانوني خاص لمواجهة هذه الظاهرة، من خلال تعريفها وتحديد خصائصها، بما يضمن حماية المعطيات والمصالح

المرتبطة باستخدام تكنولوجيات الإعلام والاتصال .ويهدف هذا المطلب إلى تسليط الضوء على مفهوم الجريمة الإلكترونية وبيان خصائصها المميزة.

الفرع الأول: تعريف الجريمة الالكترونية :

لقد تعددت الاجتهادات الفقهية بشأن تعريف الجريمة الإلكترونية، نظراً لحداثة المصطلح وتطوّر أشكال السلوك الإجرامي المرتبط باستخدام التكنولوجيا[113]. فقد عرّفها بعض الفقهاء بأنها كل فعل غير مشروع يتم باستخدام الوسائل الإلكترونية ويستهدف الأفراد أو المؤسسات بما يؤدي إلى ضرر مادي أو معنوي، في حين ركّز آخرون على الطابع الإجرائي، معتبرين أنها كل سلوك إجرامي يُرتكب من خلال الحاسوب أو الشبكة ويُعد خرقًا للقانون الجنائي، سواء تعلق الأمر بالأشخاص أو الأموال أو الأنظمة .وذهب اتجاه آخر إلى إدخال البعد الأخلاقي ضمن التعريف، حيث اعتُبرت الجريمة الإلكترونية سلوكًا غير مشروع أو غير أخلاقي يتعلق بالمعالجة الآلية للبيانات أو نقلها عبر الوسائط الرقمية .وفي ذات السياق، ترى بعض التشريعات المقارنة، كالمجلس الأوروبي ووزارة العدل الأمريكية، أن الجريمة الإلكترونية هي كل فعل يتم من خلال أو ضد نظام معلوماتي باستخدام الحاسوب أو الشبكة بقصد ارتكاب أو تسهيل جريمة[114].

وتأسيسًا على مختلف هذه الاتجاهات، يمكن اعتماد تعريف مركّب للجريمة الإلكترونية بأنها : كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال أو الأنظمة أو الحقوق المعنوية أو الخصوصية[115] .ويتميّز هذا النوع من الجرائم بطابعه التقني، وسرعة تنفيذه، واتساع نطاقه الجغرافي، ما يجعله من أخطر الجرائم المعاصرة وأكثرها تعقيدًا من حيث الإثبات والملاحقة.

وقد أولى المشرع الجزائري أهمية بالغة لموضوع الجرائم الإلكترونية، والتي أطلق عليها تسمية "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، لما لها من تأثير مباشر على الأمن العام والمصالح الحيوية للدولة. وقد اتخذت الدولة أولى خطواتها لمواجهة هذا النوع من الجرائم بإدخال تعديلات هامة على قانون العقوبات، وذلك بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، الذي عدل وأتم الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات.

وقد تضمن هذا التعديل إنشاء قسم جديد بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، حيث أُدرجت المواد من 394مكرر إلى 394 مكرر 7، والتي جرم من خلالها المشرّع مختلف الأفعال التي تمس بأنظمة المعالجة الإلكترونية للبيانات، مقدّماً عقوبات تتراوح بين سنتين إلى ثلاث سنوات حبساً، بالإضافة إلى غرامات مالية تتراوح من 50.000 دج إلى 5.000.000 دج، وذلك بحسب جسامة الجريمة وخطورتها.

---

[113] - مقلاتي مونة، مشري راضية، "الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية"، أبحاث قانونية وسياسية، المجلد 6، العدد 1، ص. 491- 8 جوان 2021. عبد العال الديربي الجرائم الالكترونية دراسة قانونية وقضائية مقارنة، المركز القومي للاصدارات القانونية الطبعة الأولى 2012 القاهرة مصر ص 40.

[114] - د. خالد عبد الحق، د. دعاء عبدالعال، الجرائم الإلكترونية والتحقيقات الجنائية، دار اليازوري العلمية، دون سنة نشر ص 14.

[115] - محمود مدين عبدالرحمن عبده، الجريمة الإلكترونية وتحديات الأمن القومي، القاهرة: المصرية للنشر والتوزيع، 2017. ص 13.

وفي سياق متصل، أصدر المشرع الجزائري القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث يعتبر أول قانون يُنظم الإطار العام لتبادل المعلومات والمعاملات الإلكترونية. وقد ورد في المادة 2 من هذا القانون تعريف للجريمة الإلكترونية، بأنها:

"جرائم المساس بأنظمة المعالجة الآلية للمعطيات كما هو محدد في قانون العقوبات، وأي جريمة أخرى تُرتكب أو يُسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

هذا التعريف يعكس رغبة المشرع في تبني صياغة مرنة ومفتوحة تمكّنه من مواكبة التطور السريع للوسائل التكنولوجية، مما يفسح المجال أمام القاضي لتقدير مدى انطباق النص على أفعال لم تكن معروفة سابقاً ولكنها أصبحت ممكنة بفعل الابتكار التقني. وبالاستناد إلى هذه المادة، يمكن تصنيف الجرائم الإلكترونية وفق القانون الجزائري إلى ثلاث فئات رئيسية:

1. جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
2. جرائم تُرتكب أو يُسهل ارتكابها بواسطة منظومة معلوماتية.
3. جرائم تُرتكب أو يُسهل ارتكابها عبر أنظمة الاتصالات الإلكترونية.

ويتّضح من هذا التصنيف أن المشرع الجزائري اختار اعتماد مفهوم واسع للجريمة الإلكترونية، فبالرغم من ارتباطها الوثيق بتكنولوجيات الإعلام والاتصال، إلا أن المجال بقي مفتوحاً لتشمل جميع الأنماط الإجرامية الجديدة التي قد تفرزها التطورات التقنية المتسارعة.

و تضمّن القانون الجزائري رقم 09-04 جملة من النصوص التي تُجرّم أفعالًا محددة تمس بأنظمة المعالجة الآلية للمعطيات، مما يتيح منها استخلاص تعريف ضمني للجريمة الإلكترونية في ضوء هذه الأحكام. حيث يُمكن القول إن الجريمة الإلكترونية، وفقًا لما يُستفاد من هذا القانون، هي : كل فعل عمدي يُرتكب عبر الوسائط التقنية للمعلوماتية والاتصال، ويهدف إلى الدخول غير المشروع إلى نظام معلوماتي، أو عرقلة سيره، أو المساس بالمعطيات المحفوظة فيه، أو استغلاله في تحقيق أغراض إجرامية، مما يشكل مساسًا بأنظمة المعالجة الآلية للمعطيات..

الفرع الثاني: خصائص الجريمة الالكترونية

تتمتع الجريمة الإلكترونية بجملة من الخصائص التي تميّزها عن الجرائم التقليدية[116]، وتجعل من مواجهتها تحديًا قانونيًا وتقنيًا مستمرًا:

-تُعد الجريمة الإلكترونية جريمة غير مادية أو افتراضية، حيث إنها تُرتكب في الفضاء الرقمي دون حاجة إلى تواجد مادي للجاني أو الضحية في مكان واحد. فمثلاً، يمكن لمجرم

[116] - . خالد عبد الحق، د. دعاء عبدالعال، المرجع السابق، ص 18. الديربيي، المرجع السابق ص 47.

إلكتروني أن يخترق بريدًا إلكترونيًا أو يسرق بيانات بطاقة مصرفية من خلال شبكة الإنترنت دون أن يقترب من الضحية فعليًا.

-كما تتسم هذه الجريمة بصعوبة اكتشافها وإثباتها، إذ لا تترك آثارًا مادية واضحة مثل البصمات أو الأدلة التقليدية، ويستعين مرتكبوها بوسائل تمويه رقمية كالشبكات الافتراضية (VPN)أو الحسابات الوهمية. على سبيل المثال، قد يستخدم الجاني حاسوبًا في دولة ما لتنفيذ جريمة إلكترونية في دولة أخرى دون ترك أثر يمكن تعقبه بسهولة.

-وتتميّز الجريمة الإلكترونية بسرعة انتشارها واتساع نطاقها[117]، فقد تُحدث ضررًا شاملاً في غضون ثوانٍ معدودة. فعلى سبيل المثال، يمكن لبرمجية خبيثة (فيروس) أن تُصيب آلاف الأجهزة في دول متعددة في وقت قصير، ما يُضاعف من خطورة هذا النوع من الجرائم.

-كذلك، تُرتكب هذه الجرائم بواسطة وسائط إلكترونية وتقنية كأجهزة الحاسوب، الهواتف الذكية، وشبكات الإنترنت، ما يستوجب من مرتكبيها درجة معينة من الكفاءة التقنية. ومن الأمثلة على ذلك: شنّ هجمات إلكترونية من نوع "الحرمان من الخدمة (DDoS) "على مواقع حكومية أو اقتصادية، أو القيام بعمليات تزوير في بطاقات الدفع الإلكتروني.

-وتبرز خاصية تعدد الأطراف والمواقع ضمن هذا النوع من الجرائم، إذ غالبًا ما تكون الضحية، والجاني، والخادم الإلكتروني المستخدم في الجريمة متواجدين في دول مختلفة، مما يثير إشكالات حول تحديد الاختصاص القضائي. كمثال على ذلك، يمكن أن تُخترق قاعدة بيانات مؤسسة جزائرية من قبل فاعل مقيم في أوروبا باستخدام خادم موجود في أمريكا.

-كما أن الجرائم الإلكترونية تشهد تطورًا مستمرًا في أساليبها، بتأثير مباشر من التقدم التكنولوجي المتسارع، وهو ما يصعّب على القوانين أن تواكب هذا النسق السريع. مثال على ذلك هو ظهور أنماط إجرامية حديثة تستخدم الذكاء الاصطناعي، مثل برمجيات التزييف العميق (Deepfake)أو الهجمات المؤتمتة بواسطة الروبوتات.

وأخيرًا، فإن من خصائص هذه الجرائم ازدواجية الصفة، إذ يمكن أن تكون محلية أو عابرة للحدود[118]. فقد تستهدف الجريمة الإلكترونية أفرادًا أو مؤسسات داخل الدولة فقط، أو قد تمتد إلى خارج حدودها، كما في حالة اختراق قاعدة بيانات تابعة لدولة أجنبية من داخل الجزائر لأغراض التجسس أو الابتزاز.

المطلب الثاني: الإطار القانوني الجزائري لمكافحة الجرائم الالكترونية

في ظل التحديات المتزايدة التي تفرضها الجرائم الإلكترونية، سعى المشرّع الجزائري إلى وضع إطار قانوني شامل لمكافحتها .وقد تجسد هذا الإطار من خلال تعديل قانون العقوبات، حيث تم إدراج قسم خاص بعنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، .كما تم تعزيز هذا الإطار عبر قوانين خاصة أخرى، مثل القانون رقم 04-09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، .يهدف هذا المطلب إلى دراسة الإطار القانوني الجزائري لمكافحة الجرائم الإلكترونية، من خلال استعراض الأحكام ذات الصلة في قانون العقوبات، بالإضافة إلى القوانين الخاصة الأخرى التي تعزز هذه الحماية

الفرع الأول: المكافحة التشريعية للجرائم الإلكترونية في قانون العقوبات الجزائري

[117] - رحموني، محمد. "خصائص الجريمة الإلكترونية ومجالات استخدامها." مجلة الحقيقة للعلوم الاجتماعية والإنسانية، المجلد 16، العدد 3، 1 سبتمبر 2017، الصفحات 432.

[118] - حبايبة، ميرفت محمد .مكافحة الجريمة الإلكترونية .عمان: دار اليازوري العلمية، 2022 ص 49.

لقد فرضت التطورات التكنولوجية المتسارعة على المشرّع الجزائري تحديات جديدة، خاصة مع تصاعد حجم الجرائم الإلكترونية واتساع نطاقها وتهديدها لمختلف جوانب الحياة الفردية والمؤسساتية، بل وحتى أمن الدولة. وفي هذا السياق، جاء تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، ليكرّس لأول مرة الإطار القانوني لتجريم الأفعال الإلكترونية. فقد تضمن هذا القانون إدراج مجموعة من المواد من **394مكرر إلى 394 مكرر 7**، وذلك تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، وهو عنوان يعكس التصور التشريعي للأفعال الإجرامية التي تمسّ بنظم المعلومات. ومن خلال تحليل هذه النصوص، يمكن تصنيف الجرائم الإلكترونية في التشريع الجزائري إلى عدة فئات رئيسية، كل واحدة منها تعكس طبيعة مختلفة من الجرائم التي تستهدف الفضاء الرقمي.

أولاً: جريمة الدخول غير المشروع إلى نظم المعالجة الآلية للمعطيات

تُعدّ هذه الجريمة من أبسط صور الاعتداء على المنظومة المعلوماتية، لكنها في الوقت ذاته تشكل أساساً لباقي الجرائم الإلكترونية، إذ غالباً ما يبدأ مرتكبو الجرائم السيبرانية بعملية ولوج غير قانوني إلى النظام الإلكتروني المستهدف. وتنص **المادة 394 مكرر** من قانون العقوبات[119] على تجريم فعل الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات. ويُقصد بالغش هنا استخدام وسائل احتيالية أو تقنيات برمجية متطورة للولوج إلى النظام دون ترخيص أو صلاحية. وتشدد العقوبة إذا ترتب عن هذا الدخول تغيير أو حذف للبيانات أو اضطراب في عمل النظام، لتصل العقوبة إلى الحبس من ستة أشهر إلى سنتين، وهو ما يدل على خطورة هذه الأفعال وما قد تسببه من شلل في سير عمل المؤسسات العمومية أو الخاصة، أو انتهاك لخصوصية الأفراد.

ثانياً: جريمة التلاعب بالمعطيات الإلكترونية المخزنة أو المعالجة

تُظهر **المادة 394 مكرر 1** [120]توجهاً تشريعياً واضحاً نحو حماية سلامة المعطيات الرقمية من كل أشكال التعديل أو الحذف أو الإدخال الاحتيالي. ويعد هذا النوع من الجرائم أخطر من سابقتها، إذ أن الفعل المجرّم لا يقتصر على الولوج، بل يتعداه إلى التأثير الفعلي على محتوى البيانات. ومن أمثلة ذلك، تغيير محتوى ملفات مالية، أو تزوير مستندات رقمية رسمية، أو حذف بيانات متعلقة بملفات ضرائب أو سجلات صحية. هذا النوع من الجرائم يهدد مصداقية النظام

---

[119] - المادة 394 مكرر (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 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 لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج.

[120] - المادة 394 مكرر 1 (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها. المادة 394 مكرر 2 (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي: 1 – تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم. 2 – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

المعلوماتي ويخلق نوعاً من الفوضى في الثقة الرقمية، سواء لدى المتعاملين مع الإدارة الإلكترونية أو داخل المؤسسات الاقتصادية.

ثالثاً: جريمة إنتاج أو نشر أو تداول أدوات أو معطيات تستعمل في ارتكاب الجرائم الإلكترونية

وفقاً لما نصت عليه **المادة 394 مكرر 2**، يعاقب القانون كل من يقوم عمداً بإنشاء أو جمع أو بيع أو توزيع أدوات معلوماتية، مثل البرمجيات الخبيثة أو تطبيقات الاختراق، والتي تُستخدم كوسائل لارتكاب الجرائم المعلوماتية. ويشمل ذلك أيضاً الاتجار بكلمات السر المسروقة أو المعطيات البنكية أو المعلومات الحساسة التي قد يتم استغلالها في هجمات إلكترونية. وهذه الجريمة تعكس تطوراً في إدراك المشرع لخطورة البنية التحتية للجرائم الإلكترونية، فهي تلاحق "المجهّزين" والمموّنين الرقميين للجريمة، وليس فقط منفذيها، مما يعزز من شمولية الحماية القانونية.

رابعاً: الجرائم الموجهة ضد نظم معلومات ذات طابع سيادي أو عمومي

أولى المشرع أهمية قصوى لحماية نظم المعلومات ذات الطابع السيادي، كأنظمة الدفاع الوطني أو المؤسسات العمومية، وهو ما عبّرت عنه **المادة 394 مكرر 3** .فكلما تعلق الأمر باعتداء على نظم معلومات تابعة للدولة أو للقطاع العمومي، فإن العقوبة تتضاعف تلقائياً، نظراً لما يمثله ذلك من تهديد للأمن القومي أو السيادة الرقمية. وتشمل هذه الجرائم محاولات التجسس الإلكتروني، أو تعطيل مواقع حكومية، أو سرقة بيانات استراتيجية. وهي جرائم لا تقتصر على البعد التقني، بل تمتد إلى البعد السياسي والأمني.

من أبرز التطورات في القانون الجزائري الاعتراف بالمسؤولية الجنائية للأشخاص المعنويين (شركات، مؤسسات، منظمات)، وهو ما نصّت عليه **المادة 394 مكرر 4** .فإذا ارتُكبت جريمة معلوماتية باسم شخص معنوي أو لفائدته، فإنه يعاقب بغرامة قد تصل إلى خمسة أضعاف الغرامة المقررة على الشخص الطبيعي. ويهدف هذا النص إلى ردع الشركات التي قد توظف التكنولوجيا في أغراض مخالفة للقانون، سواء من خلال جمع بيانات دون ترخيص، أو استخدام برامج غير شرعية، أو تسهيل ارتكاب جرائم إلكترونية من خلال بنيتها التحتية الرقمية.

خامساً: جريمة التآمر أو التحضير لارتكاب جريمة معلوماتية

أبرزت **المادة 394 مكرر 5** [121]بعداً استباقياً في المعالجة القانونية، إذ جرّمت الاتفاق أو التواطؤ بين شخصين أو أكثر لارتكاب جريمة إلكترونية، حتى قبل تنفيذها. ويشترط القانون أن يكون هذا الاتفاق مجسداً بأفعال مادية، مثل التحضير التقني أو تبادل الوسائل. وهذا يعكس توجه المشرّع نحو محاصرة الجريمة في مهدها، وإعطاء أهمية كبرى للجانب الوقائي.

سابعاً: مصادرة الوسائل الإلكترونية المستخدمة وإغلاق الأماكن المرتبطة بالجريمة

[121] - المادة 394 مكرر 5 (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها.

بموجب **المادة 394 مكرر 6**، أُعطي للقاضي سلطة مصادرة الأدوات المستخدمة في الجريمة الإلكترونية، سواء كانت أجهزة أو برمجيات، إلى جانب إمكانية إغلاق المحلات أو المواقع الإلكترونية التي استُخدمت كوسيلة أو وسيلة مساعدة لارتكاب الجريمة. ويُعدّ هذا النص ترجمة عملية لمبدأ "عدم إفلات الوسائل من العقوبة"، إذ لا يقتصر الجزاء على الجاني، بل يمتد ليشمل أدوات الجريمة.

ثامناً: تجريم الشروع في الجريمة المعلوماتية

أكّدت **المادة 394 مكرر 7** على أن الشروع في ارتكاب الجنح المعلوماتية يُعاقب بنفس العقوبة المقررة للجريمة التامة، وهو توجه صارم يعكس مدى خطورة هذه الجرائم، وخصوصاً أن في البيئة الرقمية قد تكون محاولة واحدة كافية لإحداث ضرر جسيم أو تسريب هائل للبيانات.

الفرع الثاني: المكافحة التشريعية للجرائم الإلكترونية في القوانين الخاصة

لم تفِ النصوص العقابية العامة بالحماية الجزائية الكافية ضد الجرائم الإلكترونية، ما دفع المشرّع الجزائري إلى اعتماد حماية خاصة عبر جملة من النصوص القانونية التي وردت ضمن تشريعات خاصة، أبرزها القانون رقم 04-09 المؤرخ في 5 أوت 2004، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وقد عرّف المشرّع من خلال هذا القانون الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال على أنها تشمل جرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما نص عليها قانون العقوبات، بالإضافة إلى الجرائم التي تُرتكب أو يُسهّل ارتكابها باستخدام منظومات معلوماتية أو أنظمة للاتصالات الإلكترونية.

تضمّن هذا القانون كذلك أحكامًا خاصة بمراقبة الاتصالات الإلكترونية، حيث اعتبرها غير جائزة إلا بإذن صادر عن السلطة القضائية المختصة، وفي حالات محددة فقط، من بينها الأفعال الموصوفة بجرائم الإرهاب والتخريب أو تلك الماسة بأمن الدولة، إضافة إلى الحالات التي ترد فيها معلومات بشأن تهديد محتمل لمنظومة معلوماتية بما يشكل خطرًا على النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. كما أجاز القانون اللجوء إلى المراقبة الإلكترونية عندما تستدعي التحريات أو التحقيقات القضائية ذلك، لاسيما إذا تعذّر التوصل إلى نتائج دون هذه الوسيلة، وأيضًا في سياق تنفيذ طلبات التعاون القضائي الدولي المتبادل.

وفي سياق تدعيم هذه الآلية، نصّ القانون ذاته على استحداث هيئة وطنية مستقلة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وتتمتع هذه الهيئة بالشخصية المعنوية والاستقلال المالي، وتضطلع بمهام التنسيق وتنشيط الجهود الوقائية، إلى جانب مساعدة السلطات القضائية ومصالح الشرطة القضائية في مهامها، من خلال جمع المعلومات، وإنجاز الخبرات، وتبادل المعطيات مع الهيئات المماثلة في الخارج لتحديد هوية مرتكبي الجرائم ومواقعهم.

عمل المشرّع الجزائري على تعزيز الحماية القانونية في المجال الرقمي من خلال تعديل قانون حقوق المؤلف والحقوق المجاورة بموجب الأمر رقم 03-05 المؤرخ في 19 جويلية

2003[122]، حيث تم إدراج برامج الإعلام الآلي ضمن المصنفات الأصلية، مما يسمح بملاحقة كل من يعتدي عليها قضائيًا باعتبارها جرائم تمس بحقوق المؤلف. وبهذا التعديل، أصبحت الاعتداءات الرقمية على المصنفات الإلكترونية خاضعة للعقوبات الجزائية، بما يساهم في مواجهة الجرائم الإلكترونية المتعلقة بالملكية الفكرية.

كما تشمل هذه الحماية المواقع الإلكترونية التي تُستخدم لعرض المصنفات الأدبية والفنية، حيث يعتبر الموقع المسجل كمصنف خاضعًا للحماية القانونية التي تضمن لصاحبه الحق الأدبي والمالي، وتحميه من أي اعتداء كإعادة النشر أو النسخ أو التعديل غير المصرح به. كما يُجرَّم الاعتداء على العناصر المميزة للموقع، مثل الاسم التجاري أو الشعار، في حال استغلالها دون ترخيص، ما يعزز من فعالية القانون في مكافحة الاستغلال غير المشروع للهوية الرقمية.

وتمتد هذه الحماية لتشمل الحقوق الشخصية للأفراد في الفضاء الرقمي، مثل الحق في الاسم والصورة والحياة الخاصة، إذ يعد أي اعتداء عليها جريمة يعاقب عليها القانون. وعليه، فإن قانون حقوق المؤلف والحقوق المجاورة لا يقتصر فقط على حماية المصنفات، بل يشكل أيضًا أداة قانونية لمواجهة مختلف أشكال الجرائم الإلكترونية التي تمس الملكية الفكرية وحقوق الأفراد في البيئة الرقمية.

في إطار تعزيز الحماية القانونية للاتصالات الإلكترونية، أقرّ المشرّع الجزائري القانون رقم 18-04 المؤرخ في 10 مايو 2018، والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية [123].يتضمن هذا القانون أحكامًا تهدف إلى حماية سرية المراسلات الإلكترونية، حيث نصّت المادة 105 على ضرورة احترام سرية المراسلات، في حين عاقبت المادة 127 كل من يستغل بحكم مهنته إمكانية فتح أو تحويل أو تخريب البريد أو انتهاكه، بفرض عقوبات تصل إلى الحرمان من كافة الوظائف أو الخدمات العمومية لمدة تتراوح بين خمس إلى عشر سنوات.

كما أشار القانون إلى التطور في مجال التحويلات المالية الإلكترونية، حيث نصّت المادة 87 على إمكانية إجراء التحويلات المالية عبر الوسائل الإلكترونية، في حين أكدت المادة 84 (الفقرة 2) على استخدام حوالات دفع عادية أو إلكترونية أو برقية .تعكس هذه الأحكام سعي المشرّع إلى مواكبة التطور التكنولوجي وتوفير إطار قانوني ينظم العمليات المالية الإلكترونية، مع التأكيد على ضرورة احترام سرية المراسلات وحمايتها من أي انتهاك.

تجدر الإشارة إلى أن هذا القانون يعكس التزام الجزائر بتحديث تشريعاتها لمواكبة التطور التكنولوجي، وتوفير حماية قانونية للاتصالات الإلكترونية، مما يعزز الثقة في استخدام هذه الوسائل ويحد من الجرائم الإلكترونية المرتبطة بها.

ومن الناحية الإجرائية، جاء القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، المعدل لقانون الإجراءات الجزائية، بأحكام مهمة تسهّل تتبع مرتكبي الجرائم السيبرانية، حيث استحدث المحاكم الجزائية ذات الاختصاص الموسع، ومنحها صلاحية النظر في الجرائم المتعلقة بأنظمة

---

[122] - الامر رقم 03 05 مؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاوره الصادر في الجريده الرسميه للجمهوريه الجزائريه العدد 44 بتاريخ 23 يوليو 2003

[123] - القانون رقم 18-04 المؤرخ في 10 مايو 2018، والذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية. الصادر في الجريده الرسميه للجمهوريه الجزائريه العدد 27 بتاريخ 13 ماي 2018.

المعالجة الآلية للمعطيات. كما أجاز تمديد الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق والمحاكم المختصة ليشمل أماكن خارج نطاقهم الجغرافي المعتاد، كلما دعت الضرورة إلى ذلك، وذلك وفقًا لما تنص عليه المواد 37، 40 و329 من القانون.

وقد توسّع المشرّع في الصلاحيات المتعلقة بالتحري، حيث أتاح، في الحالات التي تتطلبها ضرورة التحقيق، اعتراض المراسلات عبر وسائل الاتصال السلكية واللاسلكية دون الحاجة إلى موافقة مسبقة من الأطراف المعنية، بما يتيح إمكانية التقاط وتسجيل المحادثات الخاصة، ويعزز فرص التعرف على الجناة ومتابعة تحركاتهم. ومنح القانون كذلك لوكيل الجمهورية، وتحت إشرافه، صلاحية الأمر بتنفيذ عملية "التسرب"، والتي تعني إدخال عناصر أمنية أو تقنية إلى محيط الجريمة السيبرانية بشكل غير ظاهر، بهدف جمع الأدلة وكشف هوية الفاعلين، خاصة عند تعذر الوصول إلى نتائج بالطرق التقليدية.

وفي سياق دعم الثقة في المعاملات الرقمية، أقرّ المشرّع الجزائري، من خلال القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين[124]، حماية قانونية تهدف إلى تأمين استخدام هذه التقنيات. فنصت المادة 66 من هذا القانون على معاقبة كل من يدلي بتصريحات كاذبة بغرض الحصول على شهادة تصديق إلكتروني موصوفة، لما يشكله ذلك من مساس بمصداقية نظام المصادقة. كما جرّمت المادة 68 حيازة أو إفشاء أو استعمال بيانات إنشاء التوقيع الإلكتروني الموصوف العائد للغير دون مبرر قانوني، لما ينطوي عليه ذلك من انتهاك لخصوصية وأمن المعاملات الرقمية. وشددت على ضرورة استخدام الشهادة الإلكترونية وفقًا للغرض الممنوحة من أجله، باعتبار أن استخدامها لغير هذا الغرض يُعد مخالفة يعاقب عليها القانون.

المبحث الثاني: التكنولوجيا كوسيلة لمكافحة الجريمة

أمام تنامي تعقيد الجريمة وتطور أدواتها في الفضاء الرقمي، بات من الضروري أن تُواكب المنظومة الأمنية والعدلية هذا التحول العميق من خلال تبنّي الوسائل التكنولوجية الحديثة كرافعة أساسية لتعزيز فعالية مكافحة الجريمة. ولم تعد التكنولوجيا مجرد أداة مساعدة، بل أصبحت عنصراً محورياً في مختلف مراحل العدالة الجنائية، من الوقاية والتحري إلى التحقيق وجمع الأدلة ثم الإثبات أمام القضاء.

إن تسخير الذكاء الاصطناعي، وتحليل البيانات الجنائية الضخمة، واعتماد تقنيات المراقبة الرقمية وأنظمة الأمن السيبراني، يُمثل طفرة نوعية في منظومة مكافحة الجريمة. ومع ذلك، فإن هذا التوظيف يفرض جملة من التحديات القانونية والأخلاقية الدقيقة، تتعلق بمشروعية الوسائل المستعملة وحدود التطفل على الحياة الخاصة، فضلاً عن الحاجة إلى نصوص قانونية تتماشى مع هذه التطورات المتسارعة.

من هذا المنطلق، يتناول هذا المبحث أولاً، دور التكنولوجيا في التحقيق الجنائي، وثانياً وظيفتها في الوقاية من الجريمة في محاولة لاستجلاء واقع وآفاق هذا التحول في بيئة العدالة الجنائية.

[124] - قانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكترونيين المؤرخ في 11 ربيع الثاني عام 1436 الموافق 01 فبراير سنة 2015 .

المطلب الأول: استخدام التكنولوجيا في التحقيق الجنائي

يُعَدُّ استخدام التكنولوجيا في التحقيق الجنائي تحولًا جوهريًا في منهجية البحث عن الحقيقة في العصر الرقمي .فمع تطور الجرائم الإلكترونية وتنوع أساليبها، أصبح من الضروري تبني أدوات تقنية متقدمة لضمان جمع الأدلة وتحليلها بشكل فعال .في هذا السياق، برزت الأدلة الرقمية كعنصر حاسم في إثبات الجرائم، مما استدعى من المشرع الجزائري تطوير الإطار القانوني لمواكبة هذه التحديات.

تُعَرَّف الأدلة الرقمية بأنها المعلومات والبيانات المستخرجة من الأجهزة الإلكترونية، مثل الحواسيب والهواتف الذكية، والتي يمكن استخدامها في التحقيقات الجنائية .تتميز هذه الأدلة بكونها غير ملموسة، مما يجعل جمعها وتحليلها يتطلب خبرات تقنية متخصصة .وقد أدرك المشرع الجزائري أهمية هذه الأدلة، فأصدر القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، الذي يحدد القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .

في إطار جمع الأدلة الرقمية، يُعتبر الانتقال والمعاينة من الإجراءات الأساسية، حيث يتم فحص الأجهزة الإلكترونية في مسرح الجريمة لاستخراج البيانات ذات الصلة .ويشترط القانون الجزائري الحصول على إذن قضائي لتنفيذ هذه الإجراءات، لضمان احترام الحقوق الفردية .كما يُعَدُّ التفتيش والضبط من الوسائل التقليدية لجمع الأدلة، وقد نصت المادة 5 من القانون 09-04 على إمكانية تفتيش الأنظمة المعلوماتية، بما في ذلك التفتيش عن بُعد على البيانات المخزنة داخل هذه الأنظمة.

أما فيما يتعلق بالخبرة التقنية، فقد منح المشرع الجزائري قاضي التحقيق السلطة الكاملة في اختيار الخبراء وتكليفهم بإجراء الخبرة اللازمة، وذلك وفقًا للمادة 147 من قانون الإجراءات الجزائية .ويشمل ذلك تحليل الأجهزة والبيانات المخزنة باستخدام أدوات وتقنيات متقدمة .كما أقر المشرع استخدام الشهادة المعلوماتية، حيث يُقدِّم الخبراء شهادات فنية بناءً على تحليل الأنظمة الحاسوبية والبيانات الرقمية المتعلقة بالجريمة.

فيما يتعلق بالأساليب الحديثة لجمع الأدلة الرقمية[125]، أتاح المشرع الجزائري استخدام تقنيات مثل اعتراض المراسلات، التقاط الصور، والتسجيل الصوتي، وذلك بموجب المواد 65 مكرر 5 إلى 65 مكرر 18 من قانون الإجراءات الجزائية. وتُستخدَم هذه الأساليب في حالات محددة، مثل الجرائم المنظمة، تبييض الأموال، الإرهاب، والجرائم المتعلقة بأنظمة المعالجة الآلية للمعطيات. ويشترط القانون الحصول على إذن قضائي مسبق لتنفيذ هذه الإجراءات، مع ضرورة توثيقها بشكل دقيق.

وفيما يتعلق بمراقبة الاتصالات الإلكترونية، نصت المادة 4 من القانون 09-04 على الحالات التي يجوز فيها تنفيذ هذه المراقبة، مثل مكافحة الجرائم الإرهابية والتخريبية، الاعتداء

---

[125] - محمودي، نور الهدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، المجلد 4، العدد 2، 10 جوان 2017. ، ص. 908-926
فلاك، مراد، "آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية"، مجلة الفكر القانوني والسياسي، المجلد 3، العدد 1، ، 23 سبتمبر 2019. ص. 204-219.

على الأنظمة المعلوماتية، التحقيقات القضائية، وتنفيذ طلبات المساعدة القضائية الدولية. ويشترط القانون الحصول على إذن من السلطة القضائية المختصة قبل تنفيذ هذه الإجراءات.

أخيرًا، أتاح المشرع الجزائري تفتيش المنظومات المعلوماتية وحجزها، حيث يمكن للسلطات القضائية وضباط الشرطة القضائية إجراء التفتيش على الأنظمة المعلوماتية، بما في ذلك التفتيش عن بُعد على البيانات المخزنة داخل هذه الأنظمة، وذلك بموجب المادة 5 من القانون 09-04. وعند اكتشاف معطيات تخدم التحقيق، يتم نسخها وحجزها وفقًا للقواعد المعمول بها في قانون الإجراءات الجزائية.

من خلال هذه الإجراءات والتشريعات، يتضح أن المشرع الجزائري قد أدرك أهمية الأدلة الرقمية في التحقيقات الجنائية، وسعى إلى توفير إطار قانوني يضمن جمعها وتحليلها بشكل فعال، مع الحفاظ على حقوق الأفراد وحرياته[126]م.

الفرع الثاني: استخدام الذكاء الاصطناعي في تحليل البيانات الجنائية

في ظل التطور التكنولوجي المتسارع، أصبح الذكاء الاصطناعي أداة حيوية في مجال العدالة الجنائية، حيث يُستخدم في تحليل البيانات الجنائية للكشف عن الجرائم والتنبؤ بها .وتُسهم تقنيات الذكاء الاصطناعي، مثل التعلم الآلي وتحليل البيانات الضخمة، في تعزيز فعالية التحقيقات الجنائية من خلال تحليل كميات هائلة من المعلومات بسرعة ودقة، مما يساعد في تحديد الأنماط والسلوكيات الإجرامية.

على الصعيد الدولي، بدأت العديد من الدول في وضع أطر قانونية لتنظيم استخدام الذكاء الاصطناعي في المجالات المختلفة، بما في ذلك العدالة الجنائية .فعلى سبيل المثال، وضعت بعض الدول تشريعات تُلزم بإجراء تقييمات للمخاطر المرتبطة بأنظمة الذكاء الاصطناعي، وتحديد المسؤوليات القانونية في حال حدوث أضرار نتيجة لاستخدام هذه التقنيات .

أما في الجزائر، فلا يوجد حتى الآن تشريع خاص ينظم استخدام الذكاء الاصطناعي في مجال العدالة الجنائية .ومع ذلك، فإن قانون حماية البيانات الشخصية رقم 18-07 لسنة 2018 يُعتبر خطوة نحو تنظيم استخدام التقنيات الحديثة، حيث يضع قواعد لجمع ومعالجة البيانات الشخصية، مما يؤثر بشكل غير مباشر على استخدام الذكاء الاصطناعي في هذا المجال .

في إطار تعزيز استخدام الذكاء الاصطناعي في العدالة الجنائية ومكافحة الجريمة، قامت الجزائر بخطوة استراتيجية تمثلت في إنشاء المدرسة الوطنية العليا للذكاء الاصطناعي (ENSIA)بموجب المرسوم الرئاسي رقم 21-323 المؤرخ في 22 أغسطس 2021[127] تُعنى بالتكوين العالي والبحث العلمي في هذا المجال، وتُعتبر قطب امتياز ومؤسسة ذات طابع علمي وثقافي ومهني تتمتع بالشخصية المعنوية والاستقلال المالي .فقد أدرك المشرّع الجزائري، شأنه

---

[126] - أيت عبد المالك، نادية، وفلاح، عبد القادر، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، ، 8 جانفي 2020. ص. 1689-1708
بن مالك، أحمد، والخال، إبراهيم، "دور الأدلة الرقمية في الإثبات الجنائي"، مجلة العلوم الإنسانية، المجلد 5، العدد 1، ، 10 أفريل 2021. ص. 105-122.

[127] - مرسوم رئاسي رقم 21-323 مؤ رخ في 13 محرم عام 1443 الموافق 22 غشت سنة 2021 يتضمن إنشاء مدرسة وطنية عليا للذكاء الاصطناعي.

شأن العديد من الأنظمة القانونية الحديثة، أن الذكاء الاصطناعي لا يُمثل ترفاً تقنياً، بل أداة فعالة وحاسمة في دعم عمل الأجهزة القضائية والأمنية، عبر تحليل البيانات الجنائية، التنبؤ بأنماط الإجرام، وتيسير التحقيقات المعقدة و تهدف هذه المؤسسة إلى تكوين مهندسين متخصصين في الذكاء الاصطناعي وعلوم البيانات، مع التركيز على تطوير حلول عملية ومبتكرة لمشاكل القطاعات الاجتماعية والاقتصادية المختلفة، بما في ذلك قطاع العدالة .

يتضمن برنامج ENSIA تكوينًا تحضيريًا لمدة سنتين، يليها طور ثاني يتطلب النجاح في مسابقة وطنية .يركز المنهاج على مهارات الذكاء الاصطناعي والتعلم الآلي، بالإضافة إلى التدريب العملي في مجالات مثل الروبوتات وتصميم الأنظمة الإلكترونية .كما يشمل البرنامج مواد في إدارة الأعمال وإدارة المشاريع والابتكار وريادة الأعمال، مما يعزز من قدرة الخريجين على تطبيق تقنيات الذكاء الاصطناعي في مجالات متعددة[128] .

من الناحية القانونية، تُعد هذه المبادرة خطوة نحو إدماج الذكاء الاصطناعي في منظومة العدالة الجنائية، حيث يمكن استخدام تقنيات التحليل الذكي للبيانات في التحقيقات الجنائية، مما يسهم في تحسين كفاءة وفعالية العمليات القضائية .كما أن تكوين نخبة من المهندسين المتخصصين في هذا المجال يعزز من القدرة الوطنية على مواجهة التحديات الأمنية والجريمة الإلكترونية، ويضع الجزائر في موقع متقدم في مجال الابتكار التكنولوجي .

بالتالي، فإن إنشاء ENSIA يمثل استثمارًا استراتيجيًا في رأس المال البشري، ويعكس التزام الجزائر بتطوير قدراتها في مجال الذكاء الاصطناعي، مع التركيز على تطبيقاته في العدالة الجنائية ومكافحة الجريمة، مما يعزز من سيادة القانون ويحمي المجتمع من التهديدات الأمنية المتزايدة في العصر الرقمي.

وفي هذا السياق، يصبح الاستثمار في التكوين العالي للذكاء الاصطناعي ليس فقط خطوة تعليمية، بل مطلبًا قانونيًا وأمنيا، لكون الذكاء الاصطناعي يُعزز من فعالية الإجراءات القضائية ويوفر معالجات سريعة ودقيقة للبيانات الضخمة. كما أن مشاركة المدرسة في "الجهد الوطني للبحث العلمي والتطوير التكنولوجي"، كما تنص المادة 18 من المرسوم، من شأنه دعم مشاريع تحليل الأدلة الرقمية والتنبؤ بالجريمة وإعداد خرائط ذكية للجريمة، الأمر الذي يُمكن من صياغة سياسات أمنية مبنية على المعرفة والمعطيات الواقعية، بدل الاعتماد على الآليات التقليدية فقط.

ودوليًا، يشكل إدراج الذكاء الاصطناعي ضمن منظومة العدالة مسارًا متناميًا؛ حيث أطلقت عدة دول مبادرات وطنية مماثلة مثل "الاستراتيجية الوطنية للذكاء الاصطناعي" في فرنسا، و "AI for Justice"في كندا، و"العدالة الذكية" في الصين، والتي تهدف جميعها إلى استخدام الذكاء الاصطناعي في تحسين الأداء القضائي، مكافحة الجريمة، وتسهيل الوصول للعدالة. هذه التجارب الدولية تُؤكد أن الاستثمار في الذكاء الاصطناعي في ميدان العدالة لم يعد خيارًا بل ضرورة، وتُعزز من جدوى الخطوة الجزائرية في هذا الاتجاه.

في النهاية، فإن ربط الذكاء الاصطناعي بالعدالة الجنائية لا يمكن أن يتحقق إلا من خلال إعداد كفاءات وطنية متخصصة، تتقاطع فيها المعرفة القانونية بالمهارات التقنية، وهو ما سعت

---

[128] - أسماء بليليطة، "التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر"، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، يناير 2022، ص 26متاح على/https://ijicet.journals.ekb.eg :، رقم إلكتروني: 2735-3567.

المدرسة الوطنية العليا للذكاء الاصطناعي إلى تحقيقه من خلال **منهاج تعليمي متكامل** يشمل التكوين التقني، إدارة المشاريع، المقاولاتية، والتدريب داخل المؤسسات، ليكون خريجوها جاهزين للمساهمة في تطوير منظومة العدالة الجزائرية، ودعمها بأدوات الذكاء الاصطناعي بما يتوافق مع الضوابط القانونية، وأسس العدالة وحقوق الإنسان.

المطلب الثاني: استخدام التكنولوجيا في الوقاية من الجريمة

على ضوء تطور التهديدات الإجرامية وتعقيدها في العصر الرقمي، أصبح توظيف التكنولوجيا في الوقاية من الجريمة ضرورة تفرضها طبيعة الجريمة الحديثة، لا سيما الجرائم السيبرانية، التي باتت تستهدف الأفراد والمؤسسات والدول على حد سواء. وقد أدرك المشرعون في مختلف الأنظمة القانونية، ومنها الجزائر، أهمية تقنين هذا التوجه التقني، ووضع الأطر التشريعية والتنظيمية الكفيلة بضبط استخدام التكنولوجيا في المجالات الأمنية، سواء لأغراض الرصد أو التحليل أو التنبؤ بالجرائم قبل وقوعها ..يتناول هذا المطلب الإطار القانوني لاستخدام التكنولوجيا في الوقاية من الجريمة، مع التركيز على أنظمة المراقبة وتحليل البيانات، وتقنيات التشفير والأمن السيبراني، من خلال استعراض التشريعات الوطنية الجزائرية والممارسات الدولية.

الفرع الأول: التطبيقات العملية لتوظيف التكنولوجيا في الوقاية من الجريمة

في إطار السعي لتعزيز فعالية استراتيجيات الوقاية من الجريمة، أصبح توظيف التكنولوجيا الحديثة ضرورة ملحة. تُسهم الأدوات التكنولوجية، مثل أنظمة المراقبة الذكية، وتحليل البيانات الضخمة، وتقنيات التنبؤ الإجرامي، في تمكين الجهات الأمنية من الكشف المبكر عن بؤر الإجرام والتدخل الاستباقي للحد من وقوع الجرائم مما يُساعد في توجيه الجهود الأمنية بشكل أكثر دقة وفعالية[129].

أولاً: أنظمة المراقبة وتحليل البيانات

تُعتبر أنظمة المراقبة، مثل كاميرات المراقبة وتقنيات التعرف على الوجه، أدوات فعالة في الوقاية من الجريمة. تتيح هذه الأنظمة جمع وتحليل البيانات [130]في الوقت الفعلي، مما يُمكّن السلطات من رصد الأنشطة المشبوهة والتدخل السريع عند الحاجة. ومع ذلك، يثير استخدام هذه التقنيات تساؤلات قانونية وأخلاقية، خاصةً فيما يتعلق بالخصوصية وحماية البيانات الشخصية.

على الصعيد الدولي، تُنظم قوانين مثل اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي استخدام هذه التقنيات، حيث تُفرض قيود صارمة على جمع البيانات وتخزينها، وتُشترط موافقة الأفراد المعنيين أو وجود أساس قانوني آخر لاستخدامها. وفي المملكة المتحدة، أُثيرت نقاشات حول استخدام تقنيات التعرف على الوجه في الأماكن العامة، حيث دُعيت السلطات إلى وضع ضوابط قانونية واضحة لضمان التوازن بين الأمن وحماية الحقوق الفردية

---

[129] - بوعمرة، عقبة، "التنبؤ بالجريمة في العصر الرقمي: استثمار للأنظمة الذكية في الكشف المبكر عن بؤر الإجرام"، مجلة معارف، المجلد 19، العدد 2، 22 ديسمبر 2024، الصفحات 186–204

[130] - بوعمرة، عقبة ومبرك، عبدالقادر، "الأنظمة الذكية في التقاضي الجزائي: مسألة التوازن بين السرعة وبين إشكالات التطبيق القضائي"، مجلة الدراسات القانونية، المجلد 11، العدد 1، 15 يناير 2025، الصفحات 35–55.

ثانياً: تقنيات التنبؤ الإجرامي

تُستخدم تقنيات التنبؤ الإجرامي[131] (Predictive Policing) لتحليل البيانات وتحديد المناطق والأوقات التي يُحتمل وقوع الجرائم فيها، مما يُساعد في توجيه الدوريات الأمنية بشكل أكثر فعالية. ومع ذلك، تثير هذه التقنيات مخاوف قانونية تتعلق بالتمييز والتحيز، حيث قد تُؤدي إلى استهداف مجموعات معينة بناءً على بيانات تاريخية قد تكون متحيزة.

في الاتحاد الأوروبي، يُناقش حظر استخدام هذه التقنيات في مشروع قانون الذكاء الاصطناعي(AI Act) ، حيث يُعتبر استخدامها في التنبؤ بالجريمة من التطبيقات عالية المخاطر التي تتطلب رقابة صارمة

ثالثاً: تقنيات التشفير والأمن السيبراني

تُعد تقنيات التشفير والأمن السيبراني من الركائز الأساسية في الوقاية من الجرائم الإلكترونية، حيث تسهم في حماية البيانات وتأمين البنية التحتية الرقمية. يُعتبر التشفير وسيلة فعالة لضمان سرية المعلومات، من خلال تحويل البيانات إلى رموز غير مفهومة إلا للأطراف المخولة، مما يُقلل من مخاطر التجسس والاختراق. أما الأمن السيبراني، فيشمل مجموعة من السياسات والإجراءات والتقنيات المصممة لحماية الشبكات والأنظمة والبيانات من الهجمات الإلكترونية، مما يُعزز من أمان البيئة الرقمية ويُقلل من مخاطر الجرائم الإلكترونية.

في الجزائر، أدرك المشرع أهمية مواكبة التطورات التكنولوجية، فتم سن قانون رقم 15-04 المؤرخ في 1 فبراير 2015، الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين. يهدف هذا القانون إلى تنظيم استخدام التوقيع الإلكتروني والتصديق عليه، من خلال تحديد الشروط والضوابط اللازمة لضمان صحته وحجيته القانونية. كما يُنظم القانون عمل مؤدي خدمات التصديق الإلكتروني، الذين يُعتبرون طرفًا ثالثًا موثوقًا يقوم بإصدار شهادات التصديق الإلكتروني، مما يُضفي الثقة على التعاملات الإلكترونية ويُعزز من أمان البيئة الرقمية[132].

الفرع الثاني: الإطارالقانوني لتوظيف التكنولوجيا في منع الجرائم

في ظل التطورات المتسارعة التي يشهدها العالم الرقمي، لم يعد من الممكن التصدي للظواهر الإجرامية بالأساليب التقليدية وحدها، بل أصبح توظيف التكنولوجيا في صلب السياسات الأمنية والقانونية ضرورة حتمية تفرضها طبيعة التحديات المعاصرة. ولضمان استخدام هذه الوسائل الحديثة بطريقة مشروعة ومنضبطة، كان لا بد من إرساء إطار قانوني وتشريعي واضح

---

[131] - مراد محمد غالب محمد قاسم، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة مقارنة"، المجلة العصرية للدراسات القانونية، الكلية العصرية الجامعية – رام الله – فلسطين، المجلد 2، العدد 2، يونيو 2024، الصفحات 90–114

[132] - قرواش، رضوان، "هيئات التصديق الإلكتروني في ظل القانون 15-04 المتعلق بالقواعد العامة للتوقيع والتصديق الإلكترونيين (المفهوم والالتزامات)"، مجلة الآداب والعلوم الاجتماعية، المجلد 14، العدد 1، 1 يونيو 2017، الصفحات 410–425. تبوب، فاطمة الزهراء، "التوقيع والتصديق الإلكترونيين في ظل القانون رقم 15-04 المؤرخ في أول فبراير 2015"، مجلة الدراسات القانونية، المجلد 29، العدد 2، 20 جوان 2016، الصفحات 311–328.

ومتكامل ينظم عمليات استخدام التكنولوجيا في مكافحة الجريمة والوقاية منها، ويحمي في الوقت ذاته الحقوق والحريات الأساسية للأفراد.

وعلى المستوى الدولي، فتُعد الاتفاقيات متعددة الأطراف، مثل اتفاقية بودابست بشأن الجرائم السيبرانية (2001(، نموذجًا للتشريع الدولي الذي يُنظم توظيف التكنولوجيا في مكافحة الجريمة. وتدعو هذه الاتفاقية إلى مواءمة التشريعات الوطنية مع مقتضياتها، وتعزيز التعاون القضائي والأمني عبر الحدود، وتبادل المعلومات ذات الصلة بالتهديدات الرقمية. وقد شكّلت هذه الاتفاقية مرجعًا للعديد من الدول في وضع قوانين داخلية تُتيح استخدام الوسائل التقنية في الوقاية من الجرائم، مع مراعاة المبادئ الدولية لحقوق الإنسان.

ودوليا يشهد استخدام التكنولوجيا في الوقاية من الجريمة تطورًا ملحوظًا، حيث تسعى الدول والمنظمات إلى وضع أطر قانونية تُنظّم هذا الاستخدام .في الاتحاد الأوروبي، تم الإعلان في ربيع عام 2021 عن مبادرة "بروم(Prüm II) "II ، والتي تهدف إلى توسيع نطاق تبادل المعلومات بين الدول الأعضاء، بما في ذلك صور الوجوه ومعلومات من رخص القيادة [133].وقد تم توقيع الاتفاقية من قبل البرلمان الأوروبي والمجلس في 14 مارس 2024، ونُشرت في الجريدة الرسمية للاتحاد الأوروبي في 5 أبريل 2024، مع مشاركة دول مثل أيرلندا، بينما لم تشارك الدنمارك بسبب تحفظاتها [134].

في المملكة المتحدة، تُستخدم تقنية التعرف على الوجه في الأماكن العامة لتعزيز الأمن .وقد تم إنشاء منصب مفوض القياسات الحيوية وكاميرات المراقبة بموجب قانون حماية الحريات لعام 2012، بهدف مراجعة استخدام الشرطة للبيانات البيومترية وضمان الامتثال لمدونة ممارسات كاميرات المراقبة .كما تم دمج هذا المنصب في فبراير 2022 لتعزيز الرقابة على استخدام تقنيات التعرف على الوجه.

أما في الولايات المتحدة، فتُطبق تقنيات "التنبؤ الإجرامي (Predictive Policing) "التي تعتمد على تحليل البيانات لتحديد المناطق والأوقات التي يُحتمل وقوع الجرائم فيها، مما يُساعد في توجيه الدوريات الأمنية بشكل أكثر فعالية .ومع ذلك، تواجه هذه التقنيات تحديات قانونية، حيث رفعت عدة ولايات، مثل إلينوي وكاليفورنيا ونيويورك، دعاوى قضائية ضد شركات مثل Clearview AI، متهمة إياها بانتهاك قوانين الخصوصية من خلال جمع بيانات بيومترية دون موافقة الأفراد.

أما على الصعيد الوطني، بادرت الجزائر إلى مواكبة هذه التحولات من خلال سنّ جملة من القوانين والمراسيم التي تؤطر استعمال الوسائل التكنولوجية لأغراض أمنية، سواء على مستوى الوقاية أو التحري أو الإثبات. ومن أبرز هذه النصوص نجد قانون الإجراءات الجزائية، الذي شهد تعديلات هامة سمحت باستخدام الوسائل التقنية، كالتسجيلات الصوتية والمرئية، والمراقبة الإلكترونية، والتنصت على الاتصالات، وذلك ضمن إجراءات محددة تتطلب إذنًا قضائيًا يضبط

---

[133] - فرانسوا ماينز، :Clearview AI»كيف تقوم شركة بجمع ملايين الصور بشكل غير قانوني لخدمة قوات الأمن»، نُشر في موقع نوميراما، 20 يناير 2020، متاح على:
https://www.numerama.com

[134] -https://fr.wikipedia.org/wiki/Clearview_AI

نطاقها الزمني والمكاني، بما يضمن تحقيق التوازن بين فعالية الإجراءات واحترام ضمانات المحاكمة العادلة وحقوق الخصوصية.

ومن جهة أخرى، أقر المشرع قانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها .يُعزز هذا القانون من استخدام التكنولوجيا في الوقاية من الجريمة، مع التأكيد على ضرورة احترام الحقوق والحريات الأساسية للمواطنين .كما تم استحداث القطب الجزائي الوطني المتخصص في مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بموجب الأمر رقم 21-11 المؤرخ في 25 أغسطس 2021، لتعزيز التخصص القضائي في هذا المجال

وفي السياق ذاته، صدر المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009، الذي يحدد قواعد الأمن المطبقة على النشاطات المتعلقة بالتجهيزات الحساسة[135]، والذي سمح باعتماد كاميرات المراقبة في الفضاءات العمومية والخاصة وفق شروط قانونية صارمة تراعي حماية الحياة الخاصة، وتلزم المؤسسات بضرورة الحصول على تراخيص من الجهات المعنية، فضلاً عن ضمان التشفير والحفظ المؤمّن للبيانات المصورة، ومنع استخدامها خارج الأغراض المصرح بها قانوناً.

إن الإطار القانوني لتوظيف التكنولوجيا في الحماية من الجرائم، سواء على الصعيد الوطني أو الدولي، يُمثل محورًا استراتيجيًا في المعركة ضد الجريمة المعاصرة. غير أن هذا التوجه، وإن كان يُعزّز من قدرات الوقاية، إلا أنه يستدعي يقظة قانونية دائمة لتفادي الانزلاق نحو انتهاك الحريات، وهو ما يفرض ضرورة تطوير التشريعات بصفة دورية، وضمان خضوع كافة الإجراءات التقنية للرقابة القضائية والإدارية.

الخاتمة :

ختاما لهذه المطبوعة توصلنا الى أنّ تكنولوجيات الإعلام والاتصال مع التطورات المتسارعة التي يعرفها العصر الرقمي، أصبحت جزءاً لا يتجزأ من الواقع القانوني، وأداة مؤثرة في بناء السياسات العامة، وإعادة تشكيل العلاقات القانونية والعدلية. ولم يعد بالإمكان اليوم فصل

[135] - في الجزائر، يُنظّم استخدام كاميرات المراقبة من خلال المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009، الذي يحدد قواعد الأمن المطبقة على النشاطات المتعلقة بالتجهيزات الحساسة. تُصنف كاميرات المراقبة ضمن التجهيزات الحساسة، ويشترط القانون الحصول على رخصة حيازة واستعمال من الوالي بعد إبداء رأي لجنة الأمن الولائية، ولا يُسمح ببيعها إلا للأشخاص المرخص لهم قانونًا. المرسوم التنفيذي رقم 09-410 المؤرخ في 23 ذي الحجة عام 1430 الموافق 10ديسمبر سنة 2009

الممارسة القانونية عن الفهم التكنولوجي، خاصة في مجال العلوم الجنائية الذي يشهد تحولات متزايدة بفعل الجرائم الإلكترونية ووسائل الإثبات الرقمية.

ولقد حاولت هذه المطبوعة العلمية، عبر فصولها الأربعة، الإحاطة بالإشكاليات القانونية المعاصرة التي فرضتها تكنولوجيات الإعلام والاتصال في ظل التحول الرقمي المتسارع، لا سيما في البيئة القانونية والقضائية الجزائرية. فمن خلال التأسيس لمفاهيم دقيقة حول ماهية هذه التكنولوجيات، وتفكيك أبعاد الثورة الرقمية، تمهّد الدراسة لفهم أعمق للواقع القانوني الجديد الذي بات يتشكل في الفضاء الرقمي.

كما سلّطنا الضوء، في الفصل الثاني، على العلاقة الوثيقة بين تكنولوجيات الإعلام والاتصال ورقمنة الخدمات، مع التركيز على تطبيقاتها في السياق الجزائري، وما تطرحه من تحديات تشريعية ومؤسساتية. أما الفصل الثالث، فقد تضمن تحليلاً معمقاً لأثر هذه التكنولوجيات على الإثبات القانوني، من حيث الوسائل المستحدثة للإثبات الالكترونية، والتحديات المرتبطة بقبولها قضائياً، وهو ما يمثل نقطة تحول في قواعد الإثبات الكلاسيكية.

وفي الفصل الأخير، عالجنا ثنائية الجريمة الإلكترونية باعتبار التكنولوجيا عاملاً مزدوج الدور: فهي من جهة، وسيلة جديدة ومعقدة لارتكاب أفعال مجرّمة، ومن جهة أخرى، أداة فعالة لمكافحتها عبر الوسائل التقنية الحديثة، كأنظمة الذكاء الاصطناعي، والتتبع الرقمي، والتصدي للهجمات السيبرانية.

وفي ظل هذا السياق، نأمل أن تكون هذه المطبوعة سنداً علمياً مبسطاً وفعّالاً، يُرافق طلبة الماستر في تخصص القانون الجنائي، نحو اكتساب أدوات تحليل جديدة، وفهم عميق للتحولات القانونية المرتبطة بالتكنولوجيا. فهي ليست مجرد مادة معرفية، بل تمثل خطوة نحو تمكين الطلبة من تطوير نظرتهم إلى القانون كمنظومة ديناميكية، تتفاعل مع متغيرات العصر الرقمي باستمرار.

ومن هنا، يُرجى أن تُسهم هذه المطبوعة في بناء كفاءات قانونية واعية، قادرة على التفاعل مع الإشكالات الرقمية الحديثة، وتوظيف المعرفة المكتسبة في مجال تكنولوجيات الإعلام والاتصال بما يخدم الممارسة القضائية الرشيدة، ويعزز من جودة الأداء القانوني. كما نأمل أن تكون منطلقاً لمزيد من البحث والفضول العلمي، وأن تفتح المجال أمام الطلبة للتفكير في سُبل تطوير التشريعات الوطنية، بما يتماشى مع معايير العدالة الرقمية ومتطلبات السيادة القانونية في عالم متغيّر.

قائمة المصادر والمراجع:

أولا: القوانين:

1- القوانين الدولية

- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية، المعتمد رسمياً من قبل الجمعية العامة للأمم المتحدة بالقرار 162/51 بتاريخ 16 ديسمبر 1996.
- قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية، القرار رقم 80/56 الصادر بتاريخ 12 ديسمبر 2001.

• التنظيم الأوروبي رقم 2014/910 الصادر عن البرلمان الأوروبي المتعلق بتحديد الهوية الإلكترونية وخدمات الثقة في المعاملات الإلكترونية. الصادر بتاريخ 23 يوليو 2014.

2- القوانين الوطنية:

• القانون رقم 06-02 المؤرخ في 20 فيفري 2006، المتعلق بتنظيم مهنة الموثق، الجريدة الرسمية عدد 14، مؤرخة في 08 مارس 2006، ص 15.

• قانون الإجراءات المدنية والإدارية الجزائري رقم 08-09 المؤرخ في 25 فيفري 2008، الجريدة الرسمية عدد 21، 23 أفريل 2008، ص 13.

• القانون رقم 09-04 المؤرخ في 5 أغسطس 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، تاريخ 16 أوت 2009، ص 05.

• القانون رقم 14-08 المتضمن تعديل قانون الحالة المدنية رقم 70-20، المؤرخ في 09 أوت 2014، الجريدة الرسمية عدد 49، 20 أوت 2014.

• القانون رقم 17-03 المتضمن تعديل قانون الحالة المدنية، الصادر بتاريخ 10 يناير 2017، الجريدة الرسمية عدد 02، 11 يناير 2017.

• القانون رقم 18-04 المؤرخ في 10 مايو 2018 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية، منشور بالجريدة الرسمية عدد 27 بتاريخ 13 ماي 2018.

• القانون رقم 15-03 المتعلق بعصرنة العدالة، الصادر في 1 فبراير 2015، الجريدة الرسمية العدد 06، 10 فبراير 2015.

• القانون رقم 15-04 المؤرخ في 1 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية العدد 6، فبراير 2015.

• القانون رقم 18-05 المؤرخ في 10 مايو 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية رقم 28 بتاريخ 16 ماي 2018.

• القانون رقم 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية رقم 34 بتاريخ 13 يونيو 2018.

• القانون رقم 20-04 المؤرخ في 30 مارس 2020، المتعلق بتنظيم الاتصالات الراديوية، الجريدة الرسمية، 21 أبريل 2020.

• القانون العضوي رقم 23-14 المؤرخ في 27 غشت 2023، المتعلق بالإعلام، الجريدة الرسمية عدد 77، 02 ديسمبر 2023.

• القانون رقم 23-19 المؤرخ في 2 ديسمبر 2023، المتعلق بالصحافة المكتوبة والصحافة الإلكترونية، الجريدة الرسمية عدد 77، 02 ديسمبر 2023.

• أمر رقم 75-89 المؤرخ في 30 ديسمبر سنة 1975، المتضمن قانون البريد والمواصلات.

• أمر رقم 2000-03 المؤرخ في 05 غشت سنة 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية رقم 48 المؤرخة في 06 أوت 2000.

• الأمر رقم 03-05 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، منشور بالجريدة الرسمية عدد 44 بتاريخ 23 يوليو 2003.

• مرسوم رئاسي رقم 21-323 المؤرخ في 22 غشت 2021 بإنشاء المدرسة الوطنية العليا للذكاء الاصطناعي.

• المرسوم التنفيذي رقم 09-410 المؤرخ في 10 ديسمبر 2009 المتعلق بقواعد الأمن المطبقة على النشاطات المتعلقة بالتجهيزات الحساسة.
• المرسوم التنفيذي رقم 15-3015 المؤرخ في 10 ديسمبر 2015، المتعلق بإصدار نسخ وثائق الحالة المدنية بطريقة إلكترونية، الجريدة الرسمية عدد 68، 27 ديسمبر 2015.
• المرسوم التنفيذي رقم 16-142 الصادر بتاريخ 05 ماي 2016 المحدد لكيفيات حفظ الوثيقة الموقعة إلكترونياً، منشور بالجريدة الرسمية عدد 28 بتاريخ 08 ماي 2016.
• القرار المؤرخ في 26 ديسمبر 2011، المحدد لتاريخ تداول جواز السفر الوطني البيومتري الإلكتروني، الجريدة الرسمية عدد 01، 14 جانفي 2011.

ثانياً: الكتب:

• إبراهيم عبد الله الزبيدي، العلاقات العامة والإعلام الرقابي، دار غيداء للنشر والتوزيع، 2017.
• إبراهيم عمر يحياوي، تأثير تكنولوجيا الإعلام والاتصال على العملية التعليمية في الجزائر، دار اليازوري، 2019.
• أيمن سعد سليم، التوقيع الإلكتروني، دار النهضة العربية، القاهرة، 2004.
• أيمن عبد الله فكري، الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، الطبعة الأولى، 2014.
• جمال عبد الرحمن محمد علي، الحجية القانونية للمستندات الإلكترونية، بدون دار للنشر، 2004.
• حيدر شاكر البرزنجي، محمود حسن جمعة، تكنولوجيا ونظم المعلومات في المنظمات المعاصرة، منظور إداري تكنولوجي، .2013
• خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 2020.
• خالد ممدوح إبراهيم، الإثبات الإلكتروني في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية.
• خليل صابات، جما عبد العظيم، وسائل الاتصال: نشأتها وتطورها، مكتبة الأنجلو المصرية.
• د. خالد عبد الحق ود. دعاء عبد العال، الجرائم الإلكترونية والتحقيقات الجنائية، دار اليازوري العلمية، دون سنة نشر.
• سعد غالب ياسين، الإدارة الإلكترونية، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2010، الطبعة الأولى.
• عادل عبد العزيز صالح الرشيد، قرائن الجريمة الإلكترونية وأثرها في الإثبات، دار كنوز إشبيليا للنشر والتوزيع، المملكة العربية السعودية، 2022.
• عامر إبراهيم القندلجي، الإعلام والمعلومات والإنترنت، عمان: دار اليازوري العلمية للنشر والتوزيع، 2013.
• عامر إبراهيم قنديلجي، إيمان فاضل السامرائي، تكنولوجيا المعلومات وتطبيقاتها، الطبعة الأولى، الوراق للنشر والتوزيع، 2009.
• عبد الصبور عبد القوي علي مصري، التنظيم القانوني للتجارة الإلكترونية، مكتبة القانون والاقتصاد، الرياض.

- عبد العال الديربي، الجرائم الإلكترونية: دراسة قانونية وقضائية مقارنة، المركز القومي للإصدارات القانونية، القاهرة، 2012.
- عفيفي كمال، جريمة الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت.
- علي عدنان الفيل، إجراءات التحري في جمع الأدلة والتحقيق الابتدائي في الجرائم المعلوماتية، المكتب الجامعي الحديث، مصر، 2012.
- عمر عبد العزيز هلال، وسائل التواصل الاجتماعي وأحكامها في الفقه الإسلامي، دار الكتب العلمية.
- عيسات عيني، التوجه نحو الإدارة الإلكترونية في الجزائر من خلال مشروع الجزائر الإلكترونية 2013.
- الغمري محمد، الملكية الفكرية، ببلومانيا للنشر والتوزيع.
- فتحي حسين عامر، وسائل الاتصال الحديثة من الجريدة إلى الفيسبوك، .2011
- محمد أحمد كاسب خليفة، الإثبات والالتزامات في العقود الإلكترونية، دار الفكر الجامعي، الإسكندرية.
- محمد موفق الغلاييني، وسائل الإعلام وأثرها في وحدة الأمة، دار المنارة، 1985.
- محمود مدين عبد الرحمن عبده، الجريمة الإلكترونية وتحديات الأمن القومي، المصرية للنشر والتوزيع، القاهرة، 2017.
- منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر الرقمي، العبيكان للنشر، الرياض، 2024.
- منال العشري، تكنولوجيا المعلومات ورأس المال البشري: رؤية للتنمية المستدامة 2030، دار التعليم الجامعي، الإسكندرية.
- ميرفت محمد حبايبة، مكافحة الجريمة الإلكترونية، دار اليازوري العلمية، عمان، 2022.
- هالة أحمد الحسيني، دعاء هشام جمعة، الذكاء الاصطناعي وتوظيفه في المؤسسات الإعلامية، العربي للنشر والتوزيع.
- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، 1997.
- ياسر عبد الرحمن خلف، تكنولوجيا الإعلام والاتصالات، الجنادرية للتوزيع والنشر، الطبعة الأولى، 2017.

ثالثا: المقالات والأوراق العلمية:

- أحمد بن مالك وإبراهيم الخال، "دور الأدلة الرقمية في الإثبات الجنائي"، مجلة العلوم الإنسانية، المجلد 5، العدد 1، 10 أفريل 2021.
- أسماء بليليطة، "التكريس القانوني والتنظيمي للذكاء الاصطناعي في الجزائر"، المجلة الدولية للذكاء الاصطناعي في التعليم والتدريب، يناير 2022.
- أيمن مساعدة، "التوقيع الرقمي وجهات التوثيق"، مؤتمر القانون والحاسوب، جامعة اليرموك، الأردن، .2004

•بريزة بوزعيب، "الرقمنة ودورها في عصرنة التعليم العالي في الجزائر"، مجلة جودة الخدمة العمومية للدراسات السيسيولوجية والتنمية الإدارية، المجلد 05، العدد 02، 2022.
•بواشري أمينة، "الإصلاح الإداري في الجزائر: عض تجرة مرفق العدالة (1999-2017"(، مجلة، المجلد 06، العدد 01، 2018.
•بوعرقوب نعمة، سوداني أحلام، "رقمنة الخدمة العمومية بقطاع العدالة في الجزائر: المكاسب والتحديات"، مجلة الباحث للدراسات الأكاديمية، المجلد 11، العدد 1، 21 جانفي 2024.
•دحدوح منية، محاضرات مادة الاتصال في المؤسسة، كلية العلوم الإنسانية والاجتماعية، جامعة 8 ماي 1945 قالمة، السنة الجامعية 2015-2016.
•رضا هميسي، "أحكام الشاهد في الجريمة المعلوماتية"، ورقة بحثية مقدمة ضمن أعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق، جامعة بسكرة، الجزائر، .2015
•رضوان قرواش، "هيئات التصديق الإلكتروني في ظل القانون 15-04"، مجلة الآداب والعلوم الاجتماعية، المجلد 14، العدد 1، 1 يونيو 2017.
•زيد حمزة مقدم، "وسائل وضمانات التوثيق الإلكتروني"، مجلة جامعة بحري للآداب والعلوم الإنسانية، السودان، السنة الثالثة، العدد السادس، ديسمبر 2014.
•سمير شوقي، "دور الإعلان العالمي لحقوق الإنسان في تدويل حماية الشخصية الإنسانية"، مجلة تحولات، المجلد 02، العدد 01.
•الصالحين محمد العيش، "دور الدليل الإلكتروني في إثبات المعاملات المصرفية: عرض وتقييم لموقف القانون الليبي"، المؤتمر الدولي السابع عشر بجامعة الإمارات العربية المتحدة، كلية القانون، أبو ظبي، 20-19ماي 2009.
•عابد فايد عبد الفتاح فايد، "الكتابة الإلكترونية في القانون المدني: الفكرة والوظائف"، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة حلوان، مصر، 2008.
•عرابة الحاج وزرقون محمد، "عصرنة نظام الضمان الاجتماعي في الجزائر: تجربة بطاقة الشفاء"، مجلة الباحث الاقتصادي، العدد 02، 2014.
•عقبة بوعمرة وعبد القادر مبرك، "الأنظمة الذكية في التقاضي الجزائي: مسألة التوازن بين السرعة وإشكالات التطبيق القضائي"، مجلة الدراسات القانونية، المجلد 11، العدد 1، 15 يناير 2025.
•عقبة بوعمرة، "التنبؤ بالجريمة في العصر الرقمي: استثمار للأنظمة الذكية في الكشف المبكر عن بؤر الإجرام"، مجلة معارف، المجلد 19، العدد 2، 22 ديسمبر 2024.
•فاتح مزيتي، "مظاهر رقمنة مرفق العدالة وأثرها على تحسين الخدمة العمومية للمتقاضين"، مجلة بيبليوفيليا لدراسات المكتبات والمعلومات، المجلد 01، العدد 04، 2019.
•فاضلي سيد عي، "آثار التطور التكنولوجي على حماية الحق في الخصوصية في النظام الأوروبي لحماية حقوق الإنسان"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 05، العدد 02، سنة 2020.

• فاطمة الزهراء تبوب، "التوقيع والتصديق الإلكترونيين في ظل القانون رقم 15-04 المؤرخ في أول فبراير 2015"، مجلة الدراسات القانونية، المجلد 29، العدد 2، 20 جوان 2016.
• فؤاد علي البحراني، الإطار العام للتصديق الإلكتروني، الجهاز المركزي لتكنولوجيا المعلومات، 2008.
• فوزي عمارة، "اعتراض الممارسات كتسجيل الأصوات والتقاط الصور كإجراءات تحقيقية قضائية في القضايا الجزائية"، مجلة العلوم الإنسانية، العدد 33، جامعة قسنطينة 1، الجزائر، .2010
• محمد رحموني، "خصائص الجريمة الإلكترونية ومجالات استخدامها"، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، المجلد 16، العدد 3، سبتمبر 2017.
• محمودي نور الهدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، المجلد 4، العدد 2، 10 جوان 2017.
• مراد فلاك، "آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية"، مجلة الفكر القانوني والسياسي، المجلد 3، العدد 1، 23 سبتمبر 2019.
• مراد محمد غالب محمد قاسم، "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة مقارنة"، المجلة العصرية للدراسات القانونية، الكلية العصرية الجامعية – رام الله – فلسطين، المجلد 2، العدد 2، يونيو 2024.
• مقدم شبيلة، مقناني صبرينة، "تأثير الجرائم الإلكترونية على المعلومات الرقمية"، المجلة الجزائرية للأبحاث والدراسات، المجلد 03، العدد 01، 2020.
• مقلاتي مونة، مشري راضية، "الجريمة الإلكترونية: دلالة المفهوم وفعالية المعالجة القانونية"، أبحاث قانونية وسياسية، المجلد 6، العدد 1، 8 جوان 2021.
• نادية أيت عبد المالك وعبد القادر فلاح، "التحقيق الجنائي للجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2، 8 جانفي 2020.
• يحياوي إلهام، "دور الرقمنة في ترقية الخدمة العمومية بالجزائر: البطاقة الذهبية نموذجا"، مجلة التحليل والاستشراف الاقتصادي، المجلد 3، العدد 1، 2022.

رابعاً: المذكرات والأطاريح

• أحمد مسعود مريم، آليات مكافحة الجرائم الإلكترونية في ظل القانون رقم 09-04، مذكرة ماجستير، جامعة قاصدي مرباح، الجزائر، 2013.
• آلاء أحمد محمد حاج علي، التنظيم القانوني لجهات التصديق الإلكتروني، أطروحة ماجستير، جامعة النجاح الوطنية، فلسطين، 2013.
• حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.
• عائشة بن قارة، المرجع السابق.
• مساعد صالح نزال الشمري، دور السندات العادية في الإثبات: دراسة مقارنة بين القانونين الأردني والكويتي، مذكرة ماجستير، جامعة الشرق الأوسط، 2012.

خامسا: المواقع الإلكترونية والمنشورات الأخرى:

• بريد الجزائر: "ماضٍ في الانتقال نحو الرقمنة"، جريدة الرائد، 10أكتوبر 2023 .الرابط

- بياوي جلال، "التحول الرقمي في القطاع القضائي: تحول العدالة في العصر الرقمي"، جريدة البديل، 06أفريل 2025 .الرابط
- وكالة الأنباء الجزائرية: "رقمنة قطاع العدالة: سحب قرابة مليوني صحيفة سوابق قضائية عن بعد خلال سنة 2022"، أدرج يوم الجمعة 02 جوان 2023 .الرابط
- الاتجاهات العالمية في حرية التعبير وتنمية وسائل الإعلام: تركيز خاص على الوسائل الرقمية في عام 2015، منشورات اليونسكو، منظمة الأمم المتحدة للتربية والعلم والثقافة، ص 21.
- عادل عبد الصادق، البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين، منشورات المركز العربي لأبحاث الفضاء الإلكتروني، 2018، ص 39
- فرانسوا ماينز، :Clearview AI»كيف تقوم شركة بجمع ملايين الصور بشكل غير قانوني لخدمة قوات الأمن»، نوميراما، 20 يناير 2020، متاح على:https://www.numerama.com
- موقع وزارة العدل الجزائرية .الرابط، تاريخ الاطلاع: 2025/04/06.
- ويكيبيديا الفرنسية، Clearview AI، متاح على: https://fr.wikipedia.org/wiki/Clearview_AI

جامعة ابن خلدون تيارت
المجلس العلمي
كلية الحقوق والعلوم

فهرس الموضوعات:

الموضوعات	الصفحة
مقدمة:	05-01
الفصل الأول: الاطار المفاهيمي لتكنولوجيات الإعلام والاتصال	06
المبحث الأول: ماهية تكنولوجيات الإعلام والاتصال	06
المطلب الأول :مفهوم تكنولوجيات الإعلام والاتصال (ICT)	06
أولا: تعريف التكنولوجيا	07
ثانيا: تعريف تكنولوجيا المعلومات	08
ثالثا: تعريف تكنولوجيا الاعلام	09
رابعا: تعريف تكنولوجيا الاتصال	10
خامسا: تعريف تكنولوجيا الاعلام والاتصال	12
سادسا: موقف المشرع الجزائري من تحديد مفهوم تكنولوجيات الاعلام والاتصال:	12
المطلب الثاني :خصائص ووظائف تكنولوجيات الإعلام والاتصال الحديثة	13
أولا: خصائص تكنولوجيات الإعلام والاتصال الحديثة	13
ثانيا: وظائف تكنولوجيات الإعلام والاتصال الحديثة	15
المطلب الثالث: التطور التاريخي لتكنولوجيات الإعلام والاتصال	15
المبحث الثاني: الثورة الرقمية وانعكاساتها القانونية	18
المطلب الأول: الأبعاد القانونية للتحول الرقمي وحماية الحقوق في البيئة الرقمية	19
أولا: تأثير التطور التكنولوجي على حقوق الإنسان	19
ثانيا: تكنولوجيات الإعلام والاتصال وسرية البيانات	19
ثالثا: الجرائم الإلكترونية والقوانين الجنائية	20
رابعا: التجارة الإلكترونية والعقود الرقمية	20
خامسا: التحديات القانونية المرتبطة بتطور الذكاء الاصطناعي	21
المطلب الثاني: الاطار القانوني لتنظيم التكنولوجيا الرقمية	22
أولا: التشريعات الدولية والوطنية لتنظيم الجوانب القانونية لتكنولوجيات الاعلام والاتصال.	22
ثانيا: .التنظيم القانوني لتكنولوجيات الإعلام والاتصال في الجزائر	24
الفصل الثاني: تكنولوجيات الإعلام والاتصال ورقمنة الخدمات	28
المبحث الأول: مفهوم رقمنة الخدمات وإدماج تكنولوجيات الإعلام والاتصال	28
المطلب الأول: التعريف برقمنة الخدمات	28
المطلب الثاني: الأهمية والأهداف الاستراتيجية لرقمنة الخدمات في الجزائر	29
المبحث الثاني: واقع تطبيق رقمنة الخدمات في الجزائر باستخدام تكنولوجيات الإعلام والاتصال	30
المطلب الأول: واقع تطبيقات الرقمنة في القطاعات الحيوية بالجزائر	31
أولاً: رقمنة مصلحة الحالة المدنية	31
ثانيًا: رقمنة خدمات مؤسسة البريد والمواصلات	32
ثالثا: رقمنة خدمات قطاع العدالة :	33
رابعا : رقمنة قطاع التعليم العالي في الجزائر:	36

خامسا: رقمنة قطاع الضمان الاجتماعي في الجزائر:	37
المطلب الثاني: التحديات والعوائق أمام رقمنة الخدمات في الجزائر	37
المطلب الثالث: المتطلبات الأساسية لإنجاح عملية الرقمنة في الجزائر	38
الفصل الثالث: تكنولوجيات الإعلام والاتصال في المجال القانوني والقضائي	40
المبحث الأول: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني	40
المطلب الأول: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني المدني	41
الفرع الأول: الكتابة الإلكترونية كوسيلة إثبات في المعاملات الرقمية	41
أولا: مفهوم الكتابة الإلكترونية	41
ثانيا: أنواع الكتابة الالكترونية	43
ثالثا: الشروط الأساسية لقبول الكتابة الإلكترونية كدليل قانوني	45
رابعا: المساواة القانونية بين الكتابة الإلكترونية والورقية في الإثبات	46
الفرع الثاني: التوقيع الإلكتروني كوسيلة إثبات في المعاملات الرقمية	46
أولا : تعريف التوقيع الالكتروني	47
ثانيا: أنواع التوقيع الالكتروني:	47
ثالثا: الشروط الأساسية للاعتداد بالتوقيع الإلكتروني	49
رابعا: حجية التوقيع الإلكتروني في الإثبات	51
المطلب الثاني: أثر تكنولوجيات الإعلام والاتصال على الإثبات القانوني الجنائي	53
الفرع الأول: الأدلة الرقمية في الإثبات الجنائي وحجيتها أمام القضاء	54
أولا: تعريف الدليل الالكتروني الجنائي	54
ثانيا: خصائص الدليل الرقمي الجنائي :	55
ثالثا: شروط قبول الدليل الإلكتروني أمام القضاء الجنائي	56
رابعا: طرق جمع الادلة الرقمية الجنائية وموقف المشرع الجزائري منها	57
الفرع الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي	62
أولا: أنظمة الإثبات الجنائي وموقف المشرع الجزائري منها	62
ثانيا: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني	64
المبحث الثاني: دور تكنولوجيات الإعلام والاتصال في تأمين أدلة الإثبات القانونية: التصديق والحفظ الإلكترونيين	66
المطلب الاول : التصديق الإلكتروني ودوره في تعزيز حجية الإثبات المدني الرقمي	66
الفرع الاول: تعريف التصديق الالكتروني	67
الفرع الثاني: النظام لمؤدي خدمات التصديق الالكتروني	68
أولا: التعريف بمؤدي خدمات التصديق الالكتروني:	69
ثانيا: شروط ممارسة نشاط التصدق الالكتروني	69
ثالثا: التزامات مؤدي خدمات التصديق الالكتروني	70
المطلب الثاني: الحفظ الإلكتروني كآلية لضمان سلامة الإثبات المدني الرقمي	73
الفرع الأول: مفهوم الحفظ الالكتروني	74
الفرع الثاني: التنظيم التشريعي لآلية الحفظ الالكتروني	75
الفرع الثالث: الشروط المطلوبة للحفظ الالكتروني	77
الفرع الرابع: النظام القانوني لمؤدي خدمات الحفظ الالكتروني	79
أولا-المسئول عن تقديم خدمة حفظ التوقيع والكتابة الإلكترونية	80

ثانيا- التزامات مؤدي خدمات الحفظ الالكتروني	80
الفصل الرابع: تكنولوجيات الإعلام والاتصال والجريمة الإلكترونية	83
المبحث الأول: الجريمة الإلكترونية في ظل التطور التكنولوجي (التكنولوجيا كوسيلة لارتكاب الجريمة)	84
المطلب الأول: مفهوم الجريمة الالكترونية	84
الفرع الأول: تعريف الجريمة الالكترونية :	86
الفرع الثاني: خصائص الجريمة الالكترونية	87
المطلب الثاني: الإطار القانوني الجزائري لمكافحة الجرائم الالكترونية	87
الفرع الأول: المكافحة التشريعية للجرائم الإلكترونية في قانون العقوبات الجزائري	87
أولاً: جريمة الدخول غير المشروع إلى نظم المعالجة الآلية للمعطيات	88
ثانياً: جريمة التلاعب بالمعطيات الإلكترونية المخزنة أو المعالجة	88
ثالثاً: جريمة إنتاج أو نشر أو تداول أدوات أو معطيات تستعمل في ارتكاب الجرائم الإلكترونية	88
رابعاً: الجرائم الموجهة ضد نظم معلومات ذات طابع سيادي أو عمومي	88
خامساً: جريمة التآمر أو التحضير لارتكاب جريمة معلوماتية	89
ثامناً: تجريم الشروع في الجريمة المعلوماتية	89
الفرع الثاني: المكافحة التشريعية للجرائم الإلكترونية في القوانين الخاصة	89
المبحث الثاني: التكنولوجيا كوسيلة لمكافحة الجريمة	92
المطلب الأول: استخدام التكنولوجيا في التحقيق الجنائي	92
الفرع الثاني: استخدام الذكاء الاصطناعي في تحليل البيانات الجنائية	92
المطلب الثاني: استخدام التكنولوجيا في الوقاية من الجريمة	96
الفرع الأول: التطبيقات العملية لتوظيف التكنولوجيا في الوقاية من الجريمة	96
أولاً: أنظمة المراقبة وتحليل البيانات	96
ثانياً: تقنيات التنبؤ الإجرامي	97
ثالثاً: تقنيات التشفير والأمن السيبراني	97
الفرع الثاني: الإطار القانوني لتوظيف التكنولوجيا في منع الجرائم	98
الخاتمة	100
قائمة المصادر والمراجع	-101 107