وزارة التعليم العالي والبحث العلمي
جامعة يحي فارس بالمدية
كلية الحقوق والعلوم السياسية

الحقــوق الرقمـيـة فـي ظـل القــانـون الدولــي

مذكرة مقدمة ضمن متطلبات الحصول على شهادة الماستر

تخصص: القانون الدولي العام

تقديم الطلبة :

- سيد أحمد قصير
- سهيب شريفي

إشراف الأستاذة:

- د. فاطمة وماحنوس

أعضاء لجنة المناقشة:

الإسم واللقب	الجامعة	الصفة
أ.د أسامة غربي	جامعة يحي فارس بالمدية	رئيسا
د. فاطمة وامحنوس	جامعة يحي فارس بالمدية	مشرفا ومقررا
د. سمية يحياوي	جامعة يحي فارس بالمدية	عضوا مناقشا

السنــة الدراسية 2024 /2025م

إهداء

إلى من غرسا في قلبي حبّ العلم، وسهرا الليالي من أجلي
إلى من كانت دعواتهما سرّ توفيقي ونجاحي
إلى **أبي** العزيز، قدوتي في الصبر والعزيمة
وإلى **أمي** الغالية، نبع الحنان ومصدر القوة في كل لحظة

إلى **أخي و وأخواتي**، سندي الدائم، الذين لم يبخلوا عليّ بالدعم والمساندة
لكم جميعًا أهدي ثمرة هذا الجهد المتواضع، فأنتم جزء منه

وإلى **أصدقائي الأوفياء**، الذين كانوا خير رفيق في رحلة العلم
نتقاسم معًا لحظات الجد والتعب، كما الفرح والنجاح
أهدي لكم هذه المذكرة عربون محبة ووفاء
راجيا أن أكون عند حسن ظنكم دائمًا.

إهـــداء

إلى من كان وجودهم النور الذي أضاء لي دروب الحياة
إلى من علّموني أن الإرادة تصنع المستحيل، وأن الصبر طريق النجاح
إلى **أبي**، رمز العطاء بلا حدود، و**أمي**، منبع الحب والرحمة
إليكما أهدي كل حرف في هذه المذكرة، وكل لحظة تعب ترجمتها إلى إنجاز

إلى **إخوتي وأخواتي**، من كانوا لي السند حين تعثرت، والفرح حين نجحت
إلى **أصدقائي**، رفقاء الدرب الطويل، الذين تقاسموا معي لحظات الشك واليقين
إليكم كل الامتنان، فلكم في هذا العمل نصيب لا ينسى

.هذا الإهداء لا يوفيكم حقكم، لكنه رسالة محبة وامتنان أضعها بين أيديكم

شكر وعرفان

نتقدّم بخالص الشكر وعظيم الامتنان إلى الأستاذة المشرفة **وماحنوس فاطمة** والأستاذة **شريد وسيلة**، نظير ما بذلتاه من جهد متواصل وتوجيه مستمر في مختلف مراحل إعداد هذا العمل، فقد كان لدعمهما العلمي وتوجيهاتهما القيمة الأثر الكبير في إنجاز هذه المذكرة.

كما لا يفوتنا أن نتوجّه بجزيل الشكر والتقدير إلى الأساتذة الأفاضل أعضاء لجنة المناقشة، الذين تفضّلوا مشكورين بقبول مناقشة هذا العمل، مما يشكّل لنا مصدر فخر واعتزاز.

ولا ننسى أن نعبّر عن امتناننا العميق لكل الأساتذة الذين أسهموا في تكويننا الأكاديمي طيلة مشوارنا الدراسي، فلكم منا كل الاحترام والتقدير والعرفان.

مقدمة

مقدمة:

تشكل **الحقوق التقليدية للإنسان** الأساس الذي بُني عليه القانون الدولي لحقوق الإنسان، وهي تشمل مجموعة من الحقوق المدنية والسياسية والاقتصادية والاجتماعية التي تهدف إلى صون كرامة الإنسان وضمان حريته وأمنه. وقد حظيت هذه الحقوق بحماية دولية منذ الإعلان العالمي لحقوق الإنسان عام 1948، وتكرّست في عديد من المعاهدات الدولية مثل العهد الدولي الخاص بالحقوق المدنية والسياسية، والعهد الخاص بالحقوق الاقتصادية والاجتماعية والثقافية. تشمل هذه الحقوق، على سبيل المثال، الحق في الحياة، والحرية، والأمن، والخصوصية، والتعليم، والصحة، والعمل، والمشاركة السياسية. ويُعد احترام هذه الحقوق وتكريسها في التشريعات الوطنية والتزامات الدول الدولية أحد أهم معايير سيادة القانون ومبادئ العدالة في المجتمع الدولي.

ومع تسارع التحول الرقمي في شتى المجالات، لم تعد الحقوق والحريات تقتصر على أبعادها التقليدية، بل برزت مفاهيم جديدة فرضها الواقع الرقمي، ومن أبرزها ما يُعرف بـ"الحقوق الرقمية". وتشمل هذه الحقوق مجموعة من الحريات والضمانات التي يتمتع بها الأفراد عند استخدامهم للفضاء الرقمي، مثل الحق في الخصوصية الرقمية، وحرية التعبير على الإنترنت، وأمن المعلومات، وحماية البيانات الشخصية. وتعد هذه الحقوق امتدادًا لحقوق الإنسان في العصر الرقمي، إلا أنها تتميز بطبيعة تقنية متجددة تتطلب أطرًا قانونية مرنة وحديثة.

لقد جاء اختيار موضوع "الحقوق الرقمية في ظل القانون الدولي"نتيجة لأهمية هذا المجال والذي يشهد تطورات متلاحقة بفعل الابتكار التكنولوجي، والتوسع في استخدام الإنترنت، والاعتماد المتزايد على البيانات الشخصية من قبل الحكومات والشركات على حد سواء. كما أن هذا الموضوع يتقاطع مع عدة مجالات، مما يجعله مادة خصبة للدراسة والتحليل.

كما أن اختيار هذا الموضوع ينبع من دوافع ذاتية متعددة، يأتي في مقدمتها الاهتمام الشخصي المتزايد بقضايا التحول الرقمي وآثاره على منظومة الحقوق والحريات الأساسية، وما يطرحه من إشكالات قانونية وأخلاقية معقدة. كما أن الانخراط المتزايد في الفضاء الرقمي، سواء على المستوى المهني أو الأكاديمي، أتاح لنا معاينة التحديات الحقيقية التي يواجهها الأفراد في حماية خصوصيتهم وممارسة حريتهم في التعبير داخل هذا الفضاء. وقد ساهم هذا الوعي الذاتي في بلورة رغبة أكيدة في التعمق في الإطار القانوني الدولي الذي يُفترض أن يضمن هذه الحقوق، ويُسهم في بناء بيئة رقمية عادلة وآمنة. ومن هذا المنطلق، جاء اختيارنا للموضوع كاستجابة لحاجة شخصية للبحث في الجوانب القانونية الناظمة للعالم الرقمي، وفهم مدى نجاعة المنظومة الدولية في مواكبة التطورات التكنولوجية المتسارعة.

و يسعى البحث إلى تحقيق مجموعة من **الأهداف**، أبرزها:

- تقديم تأصيل نظري لمفهوم الحقوق الرقمية وخصائصها وموقعها ضمن منظومة حقوق الإنسان.
- تحليل الإطار القانوني الدولي المنظم لهذه الحقوق، من خلال دراسة الاتفاقيات واللوائح ذات الصلة.
- إبراز أهم التحديات التي تعوق تكريس الحقوق الرقمية في الواقع، خاصة على المستوى الدولي.
- تقديم أمثلة واقعية تبرز التفاعل الدولي مع قضايا الحقوق الرقمية.

فعلى الرغم من الأهمية المتزايدة لهذا الموضوع، فقد واجه البحث **عدة صعوبات**، من بينها:

- حداثة المفاهيم المرتبطة بالحقوق الرقمية، وغياب تعريفات موحدة في بعض الحالات.
- محدودية النصوص الدولية الصريحة التي تتناول الحقوق الرقمية، مقارنة بالنصوص الخاصة بالحقوق التقليدية.
- صعوبة الوصول إلى بعض الوثائق أو الإحصاءات الرسمية المتعلقة بالانتهاكات الرقمية عالميًا.

وتكمن أهمية الموضوع في كونه يسلّط الضوء على واقع حقوق الإنسان في العصر الرقمي، ويُبرز مدى قدرة القانون الدولي على مواكبة هذه التحولات، من خلال تطوير قواعد قانونية تضمن حماية الحقوق الرقمية، والحد من الانتهاكات الناتجة عن المراقبة، أو التجسس، أو الجرائم الإلكترونية، أو استغلال البيانات من قبل الفاعلين الرقميين الكبار. كما يساهم البحث في توضيح العلاقة بين الحقوق الرقمية وغيرها من الحقوق التقليدية، وفي إبراز ضرورة وجود توازن بين الأمن والحرية في البيئة الرقمية.

وانطلاقا من أهمية الموضوع يمكن طرح الإشكالية البحث التالية:

هل يوجد إطار تنظيمي للحقوق الرقمية على المستوى الدولي يمكنه تجاوز التحديات المعاصرة التي تفرضها البيئة الرقمية؟

وتتفرع عن هذه الإشكالية عدة تساؤلات فرعية، من بينها:

- ما هي الخصائص المميزة للحقوق الرقمية؟
- ما موقع الحقوق الرقمية ضمن المنظومة الدولية لحقوق الإنسان؟
- كيف تعاملت الاتفاقيات الدولية مع مسألة الحقوق الرقمية؟
- ما أبرز التحديات التي تواجه تنفيذ هذه الحقوق على المستوى الدولي؟

سوف تتم الإجابة على هذه الإشكالية بالاعتماد على **المنهج التحليلي الوصفي**، من خلال دراسة وتحليل النصوص القانونية والاتفاقيات الدولية ذات الصلة، بهدف الوقوف على مدى استجابتها لمتطلبات حماية

الحقوق الرقمية في ظل التحولات التي يشهدها العالم الرقمي المعاصر. كما تسعى هذه الدراسة إلى **رصد التحديات الواقعية والعملية** التي تعيق تفعيل تلك الحقوق، عبر تحليل نماذج من قضايا دولية معاصرة تعكس حجم التوتر القائم بين التطور التكنولوجي المتسارع من جهة، والحاجة إلى حماية حقوق الإنسان وضمانها في البيئة الرقمية من جهة أخرى.

وبالنظر إلى تعدد محاور الموضوع وتشعباته، تم تقسيم البحث إلى فصلين رئيسيين:
يتناول الفصل الأول من هذا البحث الإطار المفاهيمي للحقوق الرقمية، حيث يُخصص لتوضيح الأسس النظرية التي يقوم عليها هذا المفهوم المستحدث. ويشمل هذا الفصل مبحثين رئيسيين؛ يُعنى المبحث الأول بتحديد ماهية الحقوق الرقمية من خلال الوقوف على تعريفها، إبراز خصائصها المميزة، وبيان أوجه التشابه والاختلاف بينها وبين الحقوق التقليدية المعروفة في القانون الدولي. أما المبحث الثاني فيتناول أهم الحقوق الرقمية التي أثارت اهتمام المجتمع الدولي، مثل الحق في الخصوصية الرقمية، وحرية التعبير عبر الوسائط الإلكترونية، والحق في الأمن السيبراني.
أما الفصل الثاني، فيتعلّق بـ الإطار القانوني للحقوق الرقمية على المستوى الدولي، ويهدف إلى تسليط الضوء على الجهود القانونية والتنظيمية التي بُذلت لحماية هذه الحقوق في البيئة الرقمية. يتضمن هذا الفصل كذلك مبحثين اثنين؛ حيث يركّز المبحث الأول على بيان الاتفاقيات واللوائح الدولية ذات الصلة، مثل العهد الدولي الخاص بالحقوق المدنية والسياسية، واتفاقية بودابست بشأن الجريمة الإلكترونية، واللائحة العامة لحماية البيانات (GDPR) المعتمدة في الاتحاد الأوروبي. في حين يتناول المبحث الثاني الجهود الدولية المبذولة لمواجهة التحديات الراهنة التي تهدد هذه الحقوق، من خلال استعراض نماذج واقعية لقضايا معاصرة تُبرز التحديات التقنية والقانونية التي تواجه المجتمع الدولي في هذا المجال.

الفصل الأول:

الإطار المفاهيمي للحقوق الرقمية

الفصل الأول: الإطار المفاهيمي للحقوق الرقمية

في ظل التطور المتسارع الذي يشهده العالم الرقمي، أصبحت الحقوق الرقمية من أبرز القضايا التي تشغل اهتمام الباحثين والمشرعين والمهتمين بحقوق الإنسان. فقد أفرزت الثورة التكنولوجية والانتشار الواسع لاستخدام الإنترنت جملة من التحديات القانونية والأخلاقية المرتبطة بكيفية حماية الأفراد وضمان تمتعهم بحقوقهم في الفضاء الرقمي، تمامًا كما يتمتعون بها في الواقع المادي.

وتتجلى أهمية الحقوق الرقمية في كونها تمس جوانب متعددة من حياة الإنسان المعاصر، سواء فيما يتعلق بحرية التعبير، الحق في الخصوصية، حرية الوصول إلى المعلومات، أو الحماية من المراقبة والتتبع غير المشروع. كما تُعدّ هذه الحقوق امتدادًا طبيعيًا لحقوق الإنسان الأساسية، لكنها تتخذ بعدًا جديدًا ومركبًا بفعل الطبيعة الخاصة للبيئة الرقمية.

وانطلاقًا من هذا السياق، يسعى هذا الفصل إلى تقديم قراءة مفاهيمية وقانونية للحقوق الرقمية، من خلال التطرق أولًا إلى ماهيتها وتحديد مفهومها وتصنيفاتها الأساسية، ثم الانتقال في مرحلة ثانية إلى استعراض الإطار القانوني الذي يحكم هذه الحقوق في القانون الدولي، مع التركيز على المرجعيات الحقوقية الدولية التي أدرجت هذه الحقوق ضمن صلب اهتماماتها.

وعليه، يتضمن هذا الفصل مبحثين رئيسيين:

المبحث الأول: مفهوم الحقوق الرقمية ويتفرع إلى ثلاث مطالب: المطلب الأول بعنوان تعريف الحقوق الرقمية والمطلب الثاني يضم خصائص الحقوق الرقمية والمطلب الثالث يضم التمييز بين الحقوق الرقمية والحقوق التقليدية.

اما المبحث الثاني: اهم الحقوق الرقمية في القانون الدولي فيضم ثلاث مطالب، المطلب الأول بعنوان الحق في الخصوصية والمطلب الثاني يتحدث عن الحق في حرية التعبير والمطلب الثالث يتحدث عن الحق في الامن السيبراني.

ويهدف هذا الفصل في مجمله إلى بناء أرضية نظرية متماسكة تُمهّد لفهم أعمق للحقوق الرقمية.

المبحث الأول: مفهوم الحقوق الرقمية

أدى التحول الرقمي الشامل الذي يشهده العالم في العقود الأخيرة إلى بروز نوع جديد من الحقوق يُعرف بالحقوق الرقمية، وهي حقوق نابعة من الاستخدام المتزايد لتكنولوجيا المعلومات والاتصال، والتي باتت تؤثر على مختلف جوانب حياة الأفراد داخل الفضاء الرقمي. وقد أصبحت هذه الحقوق ضرورة حتمية لحماية الكرامة الإنسانية وضمان ممارسة الحريات في بيئة رقمية تتسم بالسرعة والانفتاح والتعقيد.

وتأتي أهمية هذا المبحث في كونه يؤسس للإطار النظري لمفهوم الحقوق الرقمية، وذلك من خلال تحديد طبيعتها ومضمونها، والوقوف على خصائصها المميزة، ثم تمييزها عن غيرها من المفاهيم القريبة أو المتداخلة.

وعليه، يتناول هذا المبحث ثلاث مطالب أساسية:

المطلب الأول مخصص للتعريف العام للحقوق الرقمية. والمطلب الثاني يتناول أهم الخصائص التي تنفرد بها هذه الحقوق في ظل البيئة الرقمية الحديثة. أما المطلب الثالث، فيُعنى بالتمييز بين الحقوق الرقمية والحقوق التقليدية للإنسان.

المطلب الأول: تعريف الحقوق الرقمية

في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصال، برزت الحاجة إلى إعادة تعريف الحقوق والحريات بما يتلاءم مع البيئة الرقمية. فقد أصبح الأفراد يمارسون أنشطتهم اليومية عبر الفضاء الإلكتروني، مما استدعى الاعتراف بحقوق جديدة تضمن لهم الحماية والحرية في هذا المجال. ويعدّ مفهوم الحقوق الرقمية من المفاهيم الحديثة التي ظهرت استجابةً لهذا التحول، إذ يشمل مجموعة من الحقوق المرتبطة باستخدام التكنولوجيا والإنترنت. في هذا الإطار، يتناول هذا المطلب مفهوم الحقوق الرقمية

الفرع الأول: تعريف الحق لغة واصطلاحا

أولا: تعريف الحق في اللغة:

"الحق أي صح وثبت وصدق، الحق نقيض الباطل ويعني الصدق وقيل الحق الواجب الثابت فالحق صدق الحديث والحق اليقين بعد الشك وحق الشيء بمعنى وجب"(2)، كما تدل على الاستقامة

والثبوت فكلمة الحق لها معاني كثيرة وهي الاستقامة، الثبوت، الصدق، الواجب الا ان الحق أوسع من الواجب.[1]

ثانيا: تعريف الحق اصطلاحا:

الحق هو استحقاق ثابت للشخص يتمتع به بموجب القانون أو العرف أو الدين، وهو يتمثل في القدرة أو السلطة التي يخولها النظام القانوني للفرد لتحقيق مصلحة مشروعة، سواء كانت ذات طابع مادي أو معنوي. مثال على ذلك: حق الملكية، حق التعليم، وحق التعبير.

ومصطلح الحق قد يختلط ويتداخل أو يلتبس مع مصطلحات أخرى تبتعد عنه في المدلول والمعنى كمصطلح القانون، ومصطلح الواجب، والحرية، والرخصة، والسلطة ويكمن الفرق فيما يلي:

1- الحق والقانون:

هناك علقة وثيقة بين الحق والقانون، وإذا كانت قواعد القانون تنظم علقات الشخاص فإن تصادم هذه

العلقات ببعضها البعض يفرض تدخل القانون لترجيح مصلحة على مصلحة وهو ما يقتضي ترجيح والاعتراف.

بحق شخص دون غيره من الناس يكفل له سلطة واستئثار على القيمة محل الحق، والقانون هو مصدر الحقوق.

2- الحق والواجب

إذا كان الحق يرتكز على فكرة التسلط ولاستئثار لصاحب الحق فإن الوضع الطبيعي والمقابل عن لذلك أن

الجميع يقع عليهم واجب احترام هذا التسلط الذي يقرره القانون ويحميه، وإن كل اعتداء ينجم عنه توقيع

الجزاء الذي قرره القانون على الطرف المعتدي، وهذا من منطلق أن صاحب الحق يتمتع بحماية القانون،

[1]- أنظر: إسماعيل عبد الفتاح عبد الكافي، حقوق الانسان العامة في الإسلام (د ب ن) ،2006، ص 17

ومن هنا تبرز العلاقة بين الحق والواجب، فالحق استئثار يحميه القانون، بينما الواجب عبارة عن قيد أو إلتزام

على عاتق الشخص.

3- الحق والحرية:

كما سبق بيانه أن الحق جوهره الاستئثار ولا تتقرر الا لإصحاب الحق أما الحرية يتمتع بها الكافة والجميع

على قدم المساواة مثال ذلك القاعدة الدستورية التي أقرت حرية المعتقد، واعتراف المؤسس الدستوري

للفراد بهذه الحريات ل يشمل البعض دون الآخر حتى لا يكون هناك تمييز.

4- الحق والرخصة:

إذا كان الحق يقوم على فكرة التسلط والاستئثار فإن الرخصة عبارة عن خيار متروك للشخص ومثال ذلك

في مجل الهبة قد يقبل الموهوب له الهبة أو يرفضها.

.5الحق والسلطة:

السلطة هي حق إدارة الشؤون الغير الشخصية مثل سلطة الولي.

ثانيا: تعريف العالم الرقمي :

"يعرفه taylor انها تمثل الفرق بين الثبات، وهي كل ما ليس له حجم ولون ويستطيع السفر في سرعة الضوء، أي ان الرقمنة من الناحية العلمية هي نظام الكتروني يمكن بعض الأجهزة من التقاط الصور للموارد المطبوعة واتاحتها بلغة مشفرة ومن ثم تخزينها ونقلها واسترجاعها ونسخها وحتى تغييرها"(3)

وعرف الدكتور فتحي عبد الهادي الرقمنة على انها "عملية نقل او تحويل البيانات الى شكل رقمي للمعالجة بواسطة الحاسب الالي[1]

وفي النظم المعلومات عادة ما يشار الى الرقمنة على انها تحويل النص المطبوع او الصور (الصور المطبوعة، الصور الفوتوغرافية، الإيضاحات والخرائط...الخ) الى إشارات ثنائية باستخدام وسيلة للمسح الضوئي وفي الاتصالات عن بعد يقصد بالرقمنة تحويل الإشارات التناظرية المستمرة الى إشارات رقمية"[2]

الفرع الثاني: تعريف الحقوق الرقمية

عرف الكاتب محمد الطاهر الحقوق الرقمية على انها" حق الافراد في الوصول الى واستخدام الحواسيب او الأجهزة الالكترونية او البرمجية او شبكات الاتصال دون قيود. [3]

وقد توسع البعض في تعريف الحقوق الرقمية على انها حق من حقوق الانسان والتي تسمح للفرد بالوصول الى المعلومات الرقمية واستخدامها وانشاءها ونشرها والوصول الى مختلف الأجهزة كالحواسيب وغيرها من أنظمة الاتصال وكذلك الحق في شبكات البث التلفزيوني والإذاعي والرقمي والتي تكفل له الوصول الى المعلومات والاخبار والبرامج بكل اشكالها.

كما عرفها المركز العربي لتطوير الاعلام الاجتماعي وجمعية الاتصالات التقدمية الحقوق الرقمية او حقوق الانترنت بانها امتداد لحقوق الانسان في العالم الواقعي وهي حقوق معترف بها ومحمية ومروج لها بموجب القوانين والمعاهدات الدولية حيث ان نفس الحقوق التي يتمتع بها الناس في العالم الواقعي يجب ان يتمتع بها في العالم الافتراضي.

المطلب الثاني: خصائص الحقوق الرقمية

إن فهم الخصائص المميزة للحقوق الرقمية يعد خطوة ضرورية لفهم طبيعتها القانونية ومكانتها في المنظومة الحقوقية الحديثة، ولا سيما في ظل التحولات الرقمية المتسارعة التي تشهدها المجتمعات. فالحقوق الرقمية ليست مفهوماً تقنياً محضاً، بل هي امتداد طبيعي لحقوق الإنسان الكلاسيكية في بيئة رقمية جديدة، تُمارَس عبر الإنترنت ووسائط التكنولوجيا الحديثة.

---

[1]- أنظر: هاني سليمان، حقوق الإنسان وحريات الأساسية، دار الشروق للنشر والتوزيع، عمان، 2000، ص 21

[2]- انظر: نجلاء أحمد ياسين، الرقمنة وتقنياتها في المكتبات العربية، العربي للنشر والتوزيع، القاهرة عام 2012 ص 16

[3]- انظر: محمد الطاهر، الحرية الرقمية، المفاهيم الاساسية، مؤسسة حرية الرأي والتعبير، ط واحد، القاهرة، 2013 ص 5

ويتجلى تفرد هذه الحقوق من خلال جملة من السمات الجوهرية التي تميزها عن غيرها من الحقوق، سواء من حيث الإطار القانوني الذي تنتظم ضمنه، أو من حيث بعدها العالمي المرتبط بطبيعة الفضاء الرقمي، أو حتى من حيث علاقتها الوظيفية الداعمة لبقية حقوق الإنسان.

وفي هذا السياق، سنعالج في هذا المطلب ثلاث خصائص رئيسية تشكّل دعائم فهم الحقوق الرقمية:

الفرع الأول يتناول ارتباط التمتع بالحقوق الرقمية بالإقرار القانوني لها، باعتبارها حقوقا يجب أن تكرّس في التشريعات وتخضع لحماية قضائية؛ بينما يركّز الفرع الثاني على الطابع العالمي والمتطور للحقوق الرقمية، نتيجة لاختراق التكنولوجيا الحدود الجغرافية وتغير أشكال الانتهاك والحماية؛ أما الفرع الثالث، فيسلّط الضوء على كون الحقوق الرقمية هي حقوق أساسية داعمة لحقوق الإنسان، لما توفره من ضمانات فعلية لممارسة حرية التعبير، والخصوصية، والمشاركة العامة في العصر الرقمي.

الفرع الأول: ارتباط التمتع بالحقوق الرقمية بالإقرار القانوني لها

تعتبر الحقوق الرقمية من حقوق الانسان الحديثة والمعترف بها بصفة رسمية، حيث تم إقرارها ضمن الأطر القانونية المعتمدة، وتختلف هذه الحقوق عن الحقوق الطبيعية، فالحقوق الطبيعية تعتبر حقوقا نظرية ومكتسبة دون الحاجة الى نص او سند قانوني فهي غير مرتبطة بالتشريعات والقوانين، مثل الحق في الحياة والحرية، اما الحقوق الرقمية فيتدخل التشريع القانوني في تحديدها وتنظيمها وحمايتها وضمان ممارستها بشكل آمن في الفضاء الرقمي [1]

فالحقوق الرقمية هي نوع حديث من الحقوق التي ظهرت نتيجة للتطور التكنولوجي، وخاصة مع الانتشار الواسع لاستخدام الإنترنت ووسائل التواصل الرقمي. ومع ازدياد الاعتماد على العالم الرقمي في حياة الفرد اليومية، من التعليم والعمل إلى التواصل والتعبير، أصبح من الضروري حماية الأفراد في هذا الفضاء، تمامًا كما تُحمى حقوقهم في العالم الواقعي.

وتتعلق الحقوق الرقمية بعدة مجالات، منها:

-الحق في الخصوصية الرقمية :أي حماية بيانات المستخدمين من التتبع أو السرقة أو الاستخدام غير المشروع.

[1]- انظر: أحمد أبو الوفاء، الوسيط في القانون الدولي العام، دار النهضة العربية للنشر والتوزيع، طبعة 4، القاهرة، مصر، 2004 ص 765

-الحق في الوصول إلى الإنترنت :وهو يُعدّ في بعض الدول شرطًا أساسيًا لممارسة باقي الحقوق الرقمية.

-الحق في حرية التعبير على المنصات الإلكترونية.

-الحق في الأمن السيبراني :أي ضمان أن تكون الأنظمة التي يستخدمها الأفراد محمية من الهجمات الإلكترونية.

وبخلاف هذه الحقوق، هناك ما يُعرف بالحقوق الطبيعية، وهي الحقوق الأساسية التي يمتلكها كل إنسان بمجرد ولادته، دون حاجة إلى قانون أو تشريع ينص عليها. من أمثلتها:

-الحق في الحياة.

-الحق في الحرية.

-الحق في الكرامة الإنسانية.

هذه الحقوق تُعتبر "فطرية" أو "نظرية" في معناها الفلسفي، لأنها تُستمد من طبيعة الإنسان، وليس من القوانين التي يسنها المجتمع. وهي حقوق ثابتة لا تتغير باختلاف الزمان أو المكان.

أما الحقوق الرقمية، فهي ليست فطرية، بل هي حقوق مكتسبة ومعترف بها قانونيًا نتيجة للتطور الرقمي، ولذلك فهي تحتاج إلى قوانين واضحة تُحددها، وتُنظمها، وتحميها من الانتهاك. وهذا ما يفعله المشرّعون اليوم في العديد من الدول، حيث يتم إصدار قوانين بهدف حماية خصوصية البيانات، وتنظيم استخدام الإنترنت، ومنع الجرائم الإلكترونية، وضمان حرية التعبير الرقمي.

الفرع الثاني: الطابع العالمي والمتطور لهذه للحقوق الرقمية

تستمد الحقوق الرقمية طابعها العالمي من الانتشار الواسع لشبكة الانترنت والتي أصبحت متاحة على نطاق واسع في مختلف انحاء العالم، وقد ساهم توفير الانترنت في تسهيل وتلبية العديد من الاحتياجات الإنسانية المرتبطة بالحقوق الرقمية، مثل: التواصل، النشر، التصفح، المراسلة، انشاء المدونات والوصول الى معلومات وغيرها من الأنشطة الرقمية.

كما ان هناك ارتباطا وثيقا بين الحقوق الرقمية والثروة الرقمية، فمع التطور المستمر للتكنولوجيا وظهور تطبيقات وممارسات جديدة عبر شبكة الانترنت، تصبح الحاجة الى تحديد الحقوق الرقمية المرتبطة بهذه التطورات والعمل على حمايتها والاعتراف بها امرا ضروريا لابد منه وذلك لمواكبة التحولات الرقمية المتسارعة.

فالحقوق الرقمية هي امتداد طبيعي لحقوق الإنسان في العصر الرقمي، مثل الحق في حرية التعبير، والخصوصية، والوصول إلى المعلومات، ولكن ضمن فضاء إلكتروني. [1]

ومع الانتشار السريع للإنترنت في العالم، أصبحت هذه الحقوق ذات طابع عالمي، حيث يمارس الأفراد أنشطتهم الرقمية كالتواصل، النشر، التصفح، التعليم، والعمل عبر الإنترنت، ما يجعل من الضروري حمايتهم قانونيًا في هذا الفضاء.

ومن جهة أخرى، هناك ترابط وثيق بين الحقوق الرقمية و"الثروة الرقمية"، التي تشمل الأصول الرقمية مثل البيانات الشخصية، الحسابات، المحتوى المنشور، وحتى العملات الرقمية. ومع كل تطور تكنولوجي جديد كظهور الذكاء الاصطناعي أو تقنيات التشفير تظهر ممارسات رقمية جديدة تحتاج إلى تنظيم قانوني واضح يحدد حقوق المستخدمين في هذا السياق، ويمنع استغلالهم أو المساس بخصوصيتهم أو حريتهم الرقمية.

وبالتالي، فإن الحفاظ على الحقوق الرقمية لا يتوقف عند ضمان حرية الوصول إلى الإنترنت، بل يشمل أيضًا حماية الأفراد من المخاطر المرتبطة بالاقتصاد الرقمي، وتنظيم استخدام البيانات، ومواجهة الجرائم السيبرانية، وغيرها.

الفرع الثالث: الحقوق الرقمية حقوقا أساسية داعمة لحقوق الانسان

عندما اقر مجلس حقوق الانسان الاعتراف بالحقوق الرقمية اكد بوضوح انها تندرج ضمن الحقوق الترفيهية و الثانوية الداعمة للحقوق الأساسية و التي تقتضي الحماية و التنظيم على نحو جاد و متكامل، و يعد هذا التوصيف متوافقا مع طبيعة هذه الحقوق نظرا لأهميتها المتزايدة في الحياة اليومية للأفراد فقد أصبحت الحقوق الرقمية ملازمة للفرد في مختلف نشاطاته: كالتواصل و العمل و الحصول على المعلومات ، فهي اليوم تحظى باهتمام متزايد من قبل الافراد و المؤسسات مبينتا اثرها في مجالات متعددة مما جعل من الضروري تنظيمها قانونيا و حمايتها بشكل فعال[2]

تعتبر الحقوق الرقمية ذات طبيعة مزدوجة حيث تعد احد أدوات دعم حقوق الانسان الأخرى و بشتى أنواعها بل و أصبحت الحقوق الرقمية مدخل لفهم باقي الحقوق و التعرف عليها، فهي تحتل اليوم الصدارة في مجال نشر حقوق الانسان و التعليم بها و التدريب عليها، كما انها تمثل الادات الفعالة في رصد و توثيق و تبادل البيانات حول الالتزام الدولي بتلك الحقوق ، و هذا بحد ذاته يبين أهمية إعطاء الحقوق الرقمية المزيد من

[1]- انظر: مجلس حقوق الإنسان التابع للأمم المتحدة(2012) ، القرار 8/20: تعزيز وحماية والتمتع بحقوق الإنسان على الإنترنت الأمم المتحدة

[2]- انظر: وسام نعمت إبراهيم السعدي، الحقوق الرقمية وآليات الحماية المقررة لها في إطار القانون الدولي لحقوق الإنسان، كلية الحقوق، جامعة الموصل، ص 55

الاهتمام على المستوى الدولي و ادماج تلك الحقوق بشكل واضح في اطار منظومة الحقوق الدولية المعترف بها في القانون الدولي لحقوق الانسان.[1]

المطلب الثالث: التمييز بين الحقوق الرقمية والحقوق التقليدية

رغم أن الحقوق الرقمية امتداد للحقوق التقليدية من حيث الأصل والمبدأ، إلا أنها تختلف عنها جوهريًا في كيفية ممارستها، وطرق انتهاكها، ونطاق حمايتها، وهو ما يستوجب الوقوف عند أبرز أوجه التمييز بينهما.

الفرع الأول :الوسيط في ممارسة الحق

الوسيط يُعد عنصرًا جوهريًا في تكييف الحق وتحديد طبيعته. ففي الحقوق التقليدية، يُمارس الحق غالبًا ضمن فضاء مادي ملموس، كالمشاركة في الاجتماعات، أو نشر المقالات عبر الصحف الورقية، أو إلقاء الخطب في المحافل العامة. هذه الوسائط كانت تخضع لإطار قانوني واضح ومحدد تنظمه تشريعات وطنية ومراقبة مباشرة من أجهزة الدولة. أما في السياق الرقمي، فالأمر يختلف جوهريًا، إذ تتم ممارسة الحق عبر بيئة افتراضية تعتمد على الإنترنت ومنصات التواصل الاجتماعي، مثل الفيسبوك، تويتر، تيك توك وغيرها، وهي منصات تخضع لشروط استخدام داخلية لا تتبع تشريعات الدولة بالضرورة، بل تخضع لشركات خاصة وعابرة للحدود.

إضافة إلى ذلك، فإن الوسيط الرقمي يجعل من الحق أكثر عرضة للرقابة التقنية غير المرئية، كاستخدام خوارزميات لتصنيف أو حذف المحتوى، أو تعطيل حسابات بناءً على بلاغات آلية. وتُصبح الرقابة هنا غير مباشرة وغير خاضعة للمساءلة القضائية المعتادة، ما يفرّغ الحق من مضمونه دون أن يُدرك صاحبه أصل الانتهاك أو مصدره.[2]

الفرع الثاني :نطاق ممارسة الحق

مع تطور وسائل الاتصال الرقمي وتوسّع استخدام الإنترنت، لم تعد ممارسة الحقوق مقتصرة على نطاق جغرافي محدد، كما هو الحال في الحقوق التقليدية. فالحق في التعبير أو الوصول إلى المعلومات، مثلًا، لم يعد مرتبطًا فقط بالمجتمع أو الدولة التي يعيش فيها الفرد، بل أصبح ذا امتداد عالمي. إذ يمكن لأي شخص نشر فكرة أو معلومة من مكان معين، وتصل خلال لحظات إلى ملايين الأشخاص في دول وقارات متعددة، دون أي قيود مادية أو جغرافية.

---

[1]- انظر: نفس المرجع، ص 56

[2]- انظر: فتحي الفاضلي، الحقوق الرقمية في ظل المجتمع الرقمي، دار النشر الجامعية، تونس، 2021، ص. 45–47.

هذا التحول الكبير نحو العالمية أحدث مشكلة قانونية تُعرف بأزمة "الاختصاص القضائي"، حيث أصبحت الدول تواجه صعوبات في حماية مواطنيها من انتهاكات تحدث في بيئة رقمية لا تقع ضمن سيادتها المباشرة. على سبيل المثال، قد يُنتهك حق فرد في الخصوصية أو حرية التعبير عبر منصة إلكترونية تُدار من دولة أجنبية، أو تخزَّن بياناته على خوادم موجودة خارج بلده، ما يجعل من الصعب فرض القانون المحلي على هذه الجهات أو مطالبتها بالمساءلة. [1]

كما أن التأثير الاجتماعي والسياسي للحقوق الرقمية بات أكثر اتساعًا وخطورة مقارنة بالحقوق التقليدية، وذلك بسبب سرعة انتشار المحتوى الرقمي وتضاعف أثره. فقد يؤدي منشور بسيط على موقع تواصل اجتماعي إلى ردود فعل جماهيرية واسعة، أو إثارة نقاشات سياسية حادة، أو حتى اضطرابات اجتماعية في وقت قياسي، وهو ما يفرض تحديات جديدة على القوانين التي كانت تُصمم للتعامل مع تأثيرات محلية وبطيئة نسبيًا.

وبالتالي، فإن ممارسة الحقوق في الفضاء الرقمي تجاوزت قدرة الدولة التقليدية على التنظيم والرقابة، وطرحت الحاجة إلى التعاون الدولي، ووضع قوانين عابرة للحدود أو على الأقل منسقة بينها، تضمن حماية فعالة للحقوق دون الإضرار بحرية الإنترنت أو الخصوصية الرقمية. [2]

الفرع الثالث: من حيث طبيعة الانتهاكات وطرق الحماية

تختلف طبيعة الانتهاكات التي تتعرض لها الحقوق التقليدية عن تلك التي تمس الحقوق الرقمية، سواء في الوسائل المستخدمة أو في سهولة رصدها ومعالجتها. في السياق التقليدي، تنطوي الانتهاكات غالبًا على إجراءات مباشرة وعلنية، يمكن توثيقها بسهولة نسبية. فعلى سبيل المثال، عندما يُمنع الأفراد من التظاهر السلمي أو تُقيد حركتهم أو يُمنع الصحفي من نشر تقاريره في صحيفة ورقية، فإن آثار هذا الانتهاك تكون واضحة للعيان، كما يمكن تصويرها أو توثيقها كتابيًا، ما يُسهّل عملية اللجوء إلى القضاء أو مؤسسات حقوق الإنسان للمطالبة بالإنصاف.

أما في العالم الرقمي، فإن الانتهاكات تأخذ طابعًا خفيًا، معقدًا، وغالبًا ما تحدث دون علم الضحية، مما يجعل اكتشافها أو إثباتها أمرًا بالغ الصعوبة. فمثلًا، قد تُنتهك خصوصية المستخدم من خلال تعقب نشاطه على الإنترنت، أو تسجيل بياناته الشخصية وجمعها من دون إذنه، أو بيعها لأغراض تسويقية، أو حتى استخدامها سياسيًا من قبل أطراف أجنبية. وهناك أيضًا ما يُعرف بـ"الرقابة

[1]- نفس المرجع، ص47

[2]- انظر: هشام شنيتي، الحقوق الرقمية بين القانون الدولي والواقع السيبراني، مجلة القانون والسياسة، جامعة الرباط، المغرب، العدد 6، 2022، ص. 100–103.

الخوارزمية"، حيث يتم تقييد وصول المستخدم إلى المعلومات بناءً على خوارزميات غير شفافة، تؤدي إلى إظهار محتويات معينة وإخفاء أخرى وفقًا لمعايير تجارية أو سياسية، دون أن يُبلَّغ المستخدم بذلك.

تتميّز الانتهاكات التي تطال الحقوق الرقمية بأنها غالبًا غير مادية أو مرئية، مما يصعّب اكتشافها أو التصدي لها باستخدام القوانين التقليدية التي صُممت لتنظيم العلاقات الواضحة والمباشرة داخل حدود الدولة. فهذه القوانين لا تأخذ في الحسبان ممارسات مثل تتبع نشاط الأفراد على الإنترنت أو التحكم بالمحتوى من خلال خوارزميات غير معلنة. ولهذا السبب، أصبح من الضروري وضع قوانين جديدة على المستوى الوطني والدولي، تُركّز على حماية البيانات الشخصية وخصوصية المستخدمين. كما يجب أن تُجبر المنصات الرقمية على توضيح كيف تُعرض المعلومات أو تُخفى، حتى يكون المستخدم على علم بكيفية تنظيم المحتوى الذي يتلقاه. ومن المهم أيضًا تعزيز استخدام أدوات الحماية مثل التشفير، ومحاسبة الجهات غير الحكومية، وعلى رأسها شركات التكنولوجيا الكبرى، التي أصبحت تسيطر على أجزاء واسعة من الإنترنت وتمارس تأثيرًا مباشرًا على الحقوق الرقمية للأفراد في مختلف أنحاء العالم.

والمفارقة الكبرى هنا أن المعتدي لم يعد دائمًا جهة سيادية كالشرطة أو الدولة، بل قد تكون شركة خاصة، أو منظمة دولية، أو حتى مجموعة من القراصنة السيبرانيين. وهذا يجعل الضحية في وضع قانوني ضعيف، إذ يواجه خصمًا غير معروف الهوية أحيانًا، أو خارج نطاق بلده القانوني، ما يعقّد عملية الإنصاف ويضعف إمكانية الوصول إلى العدالة.[1]

[1]- انظر: فتحي الفاضلي، المرجع السابق ص 47

المبحث الثاني: انواع الحقوق الرقمية

مع تطور التكنولوجيا الرقمية، برزت مجموعة من الحقوق الجديدة تُعرف بالحقوق الرقمية، وهي امتداد للحقوق والحريات التقليدية في البيئة الافتراضية. تهدف هذه الحقوق إلى حماية الإنسان في تعامله اليومي مع الوسائط الرقمية والشبكات الإلكترونية. ويُعد الحق في الخصوصية، وحرية التعبير، والحق في النسيان الرقمي و الحق في الامن السبراني من أهم هذه الحقوق. إذ تضمن هذه الحقوق للمستخدم حرية التواصل والمشاركة، دون تعرضه للرقابة أو التهديد. وسيتناول هذا المبحث أبرز هذه الحقوق في اربع مطالب رئيسية.

المطلب الأول: الحق في حرية التعبير الرقمية

يعد الحق في حرية التعبير من أبرز الحقوق الأساسية التي كرّستها المواثيق الدولية، ويمتد هذا الحق اليوم ليشمل الفضاء الرقمي، باعتباره وسيلة رئيسية للتواصل وتبادل الآراء والمعلومات. ومع تطور التكنولوجيا وانتشار الإنترنت، ظهرت تحديات جديدة تمس ممارسة هذا الحق، مما يستوجب فهمًا دقيقًا لطبيعته وحدوده في البيئة الرقمية. ومن هذا المنطلق، يتناول هذا المطلب دراسة الحق في حرية التعبير من خلال أربعة فروع: يُعنى الفرع الأول بتعريف هذا الحق، بينما يستعرض الفرع الثاني ممارسته عبر الإنترنت، ويُخصص الفرع الثالث لبيان خصائصه المميزة في البيئة الرقمية، أما الفرع الرابع فيتناول حدود حرية التعبير في هذا الفضاء، خاصة في ظل الحاجة للتوازن بين حرية الرأي وحماية الحقوق الأخرى.

الفرع الأول: تعريف الحق في حرية التعبير الرقمية

تعد حرية التعبير الرقمية على انها ذلك الامتداد الطبيعي لحرية التعبير التقليدية، لكنها تأخذ طابعا حديثا يتلاءم مع متطلبات البيئة الرقمية فهي تشمل حق الافراد في التعبير عن آرائهم و نشر أفكارهم و استقبال معلومات ، دون رقابة تعسفية من قبل الدولة او الجهات الخاصة، باستخدام الوسائل التكنولوجية مثل المدونات، المنتديات، منصات التواصل الاجتماعي، المواقع الخاصة بالأخبار و الوسائط المتعدد، و يتميز هذا الحق في السياق الرقمي باتساع نطاقه، و تعدد اشكاله، و ارتفاع سقف التأثير الذي يتيحه لأي مستخدم.[1]

كما تعتبر الحرية الرقمية ركيزة أساسية في تشييد مجتمع رقمي ديموقراطي عادل، اذ ان هذه الحرية تسمح للأفراد بالتعبير عن آرائهم ومعتقداتهم وتوجهاتهم بحرية في الفضاء الالكتروني وتكمن أهمية هذه الحرية في قدرتها على تمكين الافراد من تبادل الأفكار والحوار دون التعرض للقمع او

[1]- انظر محمد العيساوي،حرية التعبير في البيئة الرقمية: دراسة تحليلة قانونية، دار الهدى القاهرة،2020،ص51

الحضر او التمييز بسبب معتقداتهم او انتماءاتهم، غير ان ممارسة هذه الحرية يجب ان تضل ضمن إطار احترام حقوق الاخرين وعدم انتهاك النظام العام والقوانين السارية ضمانا لتحقيق التوازن بين حرية التعبير وسلامة المجتمع الرقمي[1]

وحسب لجنة حقوق الانسان بالأمم المتحدة فان حرية التعبير تمتد لتشمل "كل أنواع وسائل التعبير الرقمي"، و تتضمن الحق في المطالبة بالمعلومات تلقيها و نقلها بغض النظر عن الحدود مما يجعل البيئة الرقمية ميدانا رئيسيا لممارسة هذا الحق [2]

الفرع الثاني: الحق في التعبير عبر الفضاء الرقمي

-يندرج هذا الحق في ضمن الحق العام في حرية التعبير

-و قد اقر مجلس حقوق الانسان أهمية حقوق التعبير ووسائط الاعلام الحرة و المستقلة و المتعددة و المتنوعة على شبكة الانترنت و خارجها، في بناء المجتمعات و الديموقراطيات يعمها السلم و لا يهمش فيها احد. [3]

فحرية التعبير اذا تعتبر واحدة من الدعائم الأساسية في مفهوم الحريات الرقمية فالمساحات التي تتيحها وسائل الاتصالات للأفراد و التجمعات في توسع دائم، هذا التطور أسس بيئة متاحة للجميع للتعبير عن آرائهم [4]

تستخدم الانترنت كمنصة لتعزيز الحرية ابداء الراي و التعبير منذ ظهور البريد الالكتروني، حيث لجأ الافراد اليه لإرسال مقالاتهم و أفكارهم و تبادلها مع معارفهم ، و مع تطور هذه الوسيلة نشأت المجموعات البريدية التي اتاحت للمستخدمين مشاركة المحتوى بشكل اكثر تنظيما، ثم ظهرت بعدها مجالات و موضوعات متنوعة. [5]

ومع بداية مرحلة الويب وتوسع مفهوم شبكة المعلومات ظهرت أدوات وتقنيات جديدة مكنت المستخدمين سهولة نشر المحتوى الذي يصنعونه ومشاركته عبر نطاق واسع، وقد برزت مدونات

---

[1]- انظر بوعافية عبد الكريم، الحقوق الرقمية في البيئة الافتراضية، دراسة قانونية ، دار المعرفة ، الجزائر 2021، ص43

[2]- لجنة حقوق الانسان للأمم المتحدة، التعليق العام رقم 39 بشأن المادة 19 من العهد الدولي الخاص بالحقوق المدنية و السياسية،2011، الفقرة 12

[3]- مجلس حقوق الانسان الدورة 44، 2020، ص12

[4]- انظر، محمد الطاهر، الحرية الرقمية، المفاهيم الأساسية، مؤسسة حرية الراي والتعبير، طبعة 1، القاهرة، 2013، ص5

[5]-أنظر: نفس المرجع، ص8

ومواقع التدوين المصغر كأدوات فعالة طورت قدرة الانترنت على خدمة حرية التعبير. لا سيما في ظل الزيادة المتواصلة في اعداد مستخدمي الشبكة [1]

وعليه يمكن اعتبار حرية التعبير في العالم الرقمي حقا فرديا يتيح لكل شخص التواصل مع الاخرين والوصول الى المعلومات والأفكار بصورها المختلفة عبر المنصات الرقمية دون الخضوع لقيود الحدود الجغرافية، كما يجب على الافراد اثناء ممارسة هذا الحق الخضوع للقوانين المتعلقة بالتحريض على العنف والكراهية والتشهير ...

الفرع الثالث: الخصائص المميزة لحرية التعبير عبر الانترنت

تتميز حرية التعبير في الفضاء الرقمي بجملة من الخصائص التي تجعلها تختلف جذريا عن مثيلاتها في الوسائط التقليدية.

أولا: اللا مركزية وانعدام الوساطة

وتعتبر من أحد السمات الأساسية التي يتميز بها التعبير الرقمي عن غيره من وسائل التعبير والاعلام التقليدية مثل الصحافة والإذاعة، ففي الفضاء الرقمي يمكن للمستخدمين نشر محتواهم مباشرة دون الحاجة الى المرور عبر المؤسسات الرقابية والهيئات التحريرية التي تفرض شروطا مسبقة او موافقات قبل النشر. هذه الخاصية تتيح طابعا تلقائيا و عفويا للمحتوى الرقمي، مما يعكس حرية اكبر في التعبير، و يتيح للجميع انتاج المحتوى و مشاركته كعملية يومية، سواءاك انو افرادا عاديين ام جهات مستقلة دون قيود تفرضها الجهات الوسيطة [2]

ثانيا العالمية في الوصول والتأثير

و تعتبر من ابرز الخصائص المميزة للتعبير في البيئة الرقمية، حيث يمكن لمنشور واحد نشر على منصة رقمية ان يصل الى الاف او حتى ملايين الافراد في مختلف انحاء العالم وذلك في وقت قياسي جدا، هذه القدرة على الانتشار السريع و الواسع تمنح التعبير الرقمي طابعا عالميا فريدا يتيح له العبور عبر الحدود الجغرافية و الثقافية بسهولة و قد اشارت منظمة اليونيسكو الى ان التاثير الناتج عن المحتو الرقمي عبر الانترنت قد تفوق في بعض الحالات تاثير وسائل الاعلام التقليدية الرسمية، لا سيم

[1]-أنظر: نفس المرجع، ص8
[2]- أنظر: اليونيسكو، حرية التعبير ووسائل الاعلام الرقمية، باريس 2021، ص 18

خلال الفترات الحرجة مثل الازمات السياسية او الاجتماعية حيث يصبح الانترنت منصة رئيسية لتبادل المعلومات و تشكيل الراي العام [1]

ثالثا: السرعة واللحظية

التفاعل الرقمي يتم في الزمن الحقيقي حيث تنشر المعلومات فور حدوثها و يتلقا الجمهور الردود مباشرة، هذه الخاصية ساهمت في جعل التعبير الرقمي اكثر ديناميكية مقارنة بالتعبير الورقي او التقليدي[2]

رابعا: إمكانية التخفي وإخفاء الهوية

وتعتبر احدى الخصائص المميزة لحرية التعبير الرقمي اذ انها تمنح للافراد فرصة التعبير عن اراءهم و أفكارهم بحرية تامة دون الحاجة للكشف عن هويتهم الاصلية، تعتبر هذه الخاصية مهمة بصفة كبيرة خاصة اذا تعلق الامر بالانظمة السياسية و الاجتماعية القمعية حيث يتمكن الافراد من مشاركة وجهات النظر خاصتهم و كذا انتقاداتهم دون خوف من الملاحقة او الانتقال، الا انه هذه الميزة قد تشكل بشكل سلبي في بعض الحالات، حيث يمكن ان يلجأ البعض الى استخدام التخفي لنشر خطاب الكراهية و التحريض او نشر المعلومات المغلوطة التي تساهم في تضليل الراي العام، مما يشكل تحديا امام تحقيق توازن بين حرية التعبير و سلامة المجتمع الرقمي. [3]

الفرع الرابع: حدود حرية التعبير في البيئة الرقمية

تتجاوز حرية التعبير في البيئة الرقمية كونها مجرد امتداد للحرية التقليدية اذ انها تشكل قفزة نوعية لطريقة ممارسة هذا الحق الأساسي، فقد أصبحت تشمل اشكالا متنوعة من التعبير مثل التدوين، التغريدات، التعليقات، مقاطع الفيديو والمحتويات التفاعلية الأخرى مما يجعلها ركيزة أساسية ضمن الحقوق الرقمية المعاصرة. هذا التوسع يفرض تحديات جديدة تتعلق بإيجاد توازن دقيق بين ضمان الحرية الكاملة للتعبير من جهة والحاجة الى تنظيم هذا الفضاء لمنع إساءة الاستخدام او التأثيرات السلبية من جهة أخرى. [4]

---

[1]- أنظر: المفوضية السامية لحقوق الانسان، تقرير حرية التعبير،2019، جنيف، ص7، متاح على الرابط: https://www.ohchr.org/ar/freedom-of-expression

[2]- نفس المرجع، ص9

[3]- انظر نصر الله خالد، الرقابة وحرية التعبير في العالم العربي، الشبكة العربية لمعلومات حقوق الانسان، بيروت، 2021، ص75

[4]- أنظر: الجمعية العامة للأمم المتحدة، تقرير المقرر الخاص المعني بحرية التعبير عبر الفضاء الرقمي، الدورة 41، 2019، الفقرة 11

أولا: مبدأ القيود المشروعة والنصوص عليها قانونا

وفقا للعهد الدولي الخاص بالحقوق المدنية و السياسية يمكن فرض قيود قانونية على حرية التعبير في حالات استثنائية محددة، على شرط ان تتوافق هذه القيود مع معايير صارمة تتضمن الحماية لهذا الحق الأساسي.يتعين ان تكون القيود مكرسة ضمن قانون واضح و دقيق يحدد نطاقها بشكل لا يترك مجالا للتفسيرات الغامضة، و ان تكون موجهة لتحقيق اهداف مشروعة مثل صون امن الوطن، الحفاظ على النظام العام، حماية الصحة العامة او الحفاظ على سمعة الافراد و حقوقهم، تشكل هذه المعايير أساسا حيويا لتنظيم حرية التعبير في البيئة الرقمية، مما يتيح وضع ظوابط متوازنة تحافظ على جوهر الحرية مع منع إساءة استخدامها او التعدي على حقوق الاخرين[1]

ثانيا: مبدأ التناسب والضرورة مع فرض القيود

وفقا للقانون الدولي يشترط ان تكون القيود الموضوعة على حريه التعبير في العالم الرقمي متناسبة مع الفرص التي يتم فرضها من اجله ولا تتعدى الحد الادنى اللازم لتحقيق هذا الهدف فمثلا لا يعتبر مقبولا حظر منصة رقميه بالكامل بسبب منشور واحد مخالف بل ينبغي ان يكون التدخل يقتصر تحديدا على معالجه المحتوى الذي يثير الاشكال مع الحفاظ على استمراريه الفضاء الرقمي كمنصة للتغيير الحر. [2]

ثالثا: التوازن مع الحقوق الرقمية الأخرى:

يجب ان لا يتم استغلال حريه التعبير واستخدامها كاداه للتعدي على الخصوصية او الإساءة للأخرين والتشويه بسمعتهم او التحريض على العنف والكراهية وعليه فان هذه الحرية تتداخل بشكل وثيق مع غيرها من الحقوق الرقمية لا سيما الحق في الخصوصية الرقمية والامن السيبراني مما يتيح لها تحقيق التوازن دقيق بين ممارسه حريه التعبير وحماية هذه الحقوق الاخرى لضمان بيئة رقمية عادلة وامنة.

رابعا: صوره حريه التعبير الرقمي في الأنظمة المقيدة:

في الدول التي تتسم بأنظمة سلطوية تمثل حريه التعبير في البيئة الرقمية عمود اساسي تمكن المواطنين من التعبير عن آرائهم ومعتقداتهم بحريه مما يجعل منها اداه حيوية للتعزيز المسائلة وتشجيع

[1]- انظر: لجنة حقوق الانسان بالأمم المتحدة، التعليق العام رقم 34، الفقرة 22، المتاح على الموقع:
https://digitallibrary.un.org/record/715606?ln=ar&v=pdf
[2]- انظر: نصر الله خالد، مرجع سابق، ص 77

المشاركة السياسية والمجتمعية ومع ذلك تواجه هذه الحرية تحديات جمع تتمثل في الممارسات القمعية مثل الرقابة الإلكترونية وحجب المواقع والمنصات الرقمية والملاحظات القانونية التي تستهدف الافراد بسبب تعبيرهم عن آرائهم مما يشكل تهديدا لهذا الحق الاساسي.

خامسا: ضرورة الحوكمة والرقابة الشفافة

تؤكد التقارير الدولية على اهميه وجود اليات واضحة لمسائله شركه التكنولوجيا عند فرضها لقيود على المحتوى او حظر المستخدمين فلا يجوز ترك حرية التعبير الرقمية رهينه لخوارزميات غير شفافة او قرارات تعسفيه صادره عن شركات خاصة. [1]

المطلب الثاني : الحق في الخصوصية وحماية البيانات

يُعدّ الحق في الخصوصية وحماية البيانات من أهم الحقوق الرقمية التي برزت بقوة في ظل الثورة التكنولوجية وانتشار استخدام الوسائط الرقمية في مختلف جوانب الحياة. فقد أضحى الأفراد يتركون كميات هائلة من المعلومات الشخصية عند تعاملهم مع الفضاء الرقمي، مما يستدعي توفير حماية قانونية فعالة تضمن عدم انتهاك خصوصيتهم أو استغلال بياناتهم دون موافقتهم. ومن هذا المنطلق، يتناول هذا المطلب دراسة شاملة لهذا الحق من خلال ثلاثة فروع رئيسية، حيث يُعنى الفرع الأول بتعريف الحق في الخصوصية في البيئة الرقمية، ويتناول الفرع الثاني تحديد محل هذا الحق وأشكاله، بينما يسلّط الفرع الثالث الضوء على العلاقة الوثيقة التي تربطه ببقية الحقوق الرقمية الأخرى، مثل الحق في حرية التعبير.

الفرع الأول: تعريف الحق في الخصوصية في الفضاء الرقمي

تم تعريف الخصوصية في البيئة الرقمية على أنها "وصف لحماية البيانات الشخصية للفرد" التي يتم تداولها وجمعها ونشرها باستخدام مختلف الوسائل الرقمية و تشمل هذه البيانات الصور الشخصية، البريد الالكتروني، الحسابات البنكية، معلومات السكن و العمل و غيرها من المعلومات التي مشاركتها من خلال التفاعل عبر الانترنت أو عن طريق استخدام الحواسيب و الهواتف الذكية أو أي وسيلة من وسائل الإتصال الرقمي عبر الشبكة الأنترنت [2]

[1]- اليونسكو: دليل حوكمة المنصات الرقمية الحفاظ على حريه التعبير والوصول للمعلومة من خلال النهج تشاركي، الطبعة الأولى، باريس، 2023 ص5

[2]- انظر: مركز هردو لدعم التعبير الرقمي، انتهاك الخصوصية الرقمية للصحافة (المهنة الصحفية و الحياة الشخصية)، القاهرة،2017،ص 5

كما لاحظت مروة زين العابدين أن الخصوصية الرقمية تتمثل في عدم الاطلاع أو استخدام البيانات الشخصية عبر الانترنت دون موافقة صريحة من الشخص المعني و هو ما يجعل هذه المسألة أخلاقية و قانونية في آن واحد[1]

كذلك يعرف الحق في الخصوصية في العصر الرقمي بأنه ذلك الحق الذي يخول للفرد حماية بياناته ومعلوماته الشخصية من المعالجة، الجمع، والاستخدام اللامشروع، كما يضمن له السيطرة على مكعلوماته الرقمية مع الوقوف في وجه كل شكل من أشكال المراقبة أو الاستغلال من قبل السلطات والجهات الخاصة بما يحقق احترام الكرامة الإنسانية والحريات الأساسية في البيئة الالكترونية [2]

استنادا على ذلك يمكننا القول بأن الحق في الخصوصية داخل الفضاء الرقمي يعتبر امتدادا لحقوق الانسان، مفاده حماية البيانات الشخصية لمستخدمي الأنترنت، خاصة في ظل التقدم الكبير في تقنيات المعلومات.

الحق في الخصوصية في المجال الرقمي هي من الحقوق الأساسية المعنية بالحماية حيث يتعلق بحماية بيانات الأفراد الشخصية ومعلوماتهم الرقمية من التدخل غير المصرح بهأ والاستغلال اللامشروع. هذا الحق يشمل ضمان سرية المعلومات الشخصية، كالبيانات المتداولة عبر الانترنت أو التخزين الرقمي، والحفاظ على استقلالية الأفراد في التحكم في معلوماتهم. [3]

أما حماية البيانات الشخصية فيعتبر فرع من فروع الحق في الخصوصية أو بمعنى آخر امتداد لهذا الحق، يتمثل في قدرة الفرد على التحكم في جمع ومعالجة وتخزين واستخدام بياناته وضمان عدم الإفصاح عنها أو إساءة استخدامها بدون موافقته الصريحة، وفقا لمبادئ الشفافية والضرورة والتناسب. [4]

[1]- أنظر: مروة زين العابدين، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي والقانون الاتفاقي الوطني، القاهرة مركز الدراسات العربية للنشر و التوزيع، ط1، 2016.

[2]- انظر: المفوضية السامية لحقوق الانسان،"الحق في الخصوصية في العصر الرقمي "، الأمم المتحدة الدورة 39 لمجلس حقوق الانسان، الوثيقة رقم HRC/39/29/أوت 2018،ص5

[3]- أنظر: غزيل عائشة، الحماية الدولية للحق في الخصوصية في المجال الرقمي، جامعة غليزان، مجلة المعيار، مجلد 27، العدد 04،ص407

[4]- أنظر: علي وهبي، الحق في حماية البيانات الشخصية، بيروت، منشورات الحلبي الحقوقية، 2003، ص60

الفرع الثاني: محل الخصوصية الرقمية

تحتل الخصوصية الرقمية موقعًا محوريًا ضمن منظومة الحقوق الرقمية، كونها تتعلق بحماية البيانات الشخصية للمستخدمين في الفضاء الإلكتروني. فهي تمثل الدرع الأول ضد التتبع والتجسس وانتهاك الحياة الخاصة. ومن ثم، تُعد ضمانة أساسية لصون حرية الفرد وكرامته في العصر الرقمي.

أولا: تعريف البيانات الشخصية

تعرف البيانات الشخصية على أنها أي معلومة بغض النظر عن شكلها و مصدرها يمكن استخدامها للتعرف على هوية المستخدم بشكل دقيق سواءا كان ذلك بصورة مباشرة أو غير مباشرة.و تشمل هذه المعلومات على سبيل المثال: الأسماء، أرقام الهويات الشخصية، العناوين،أرقام التواص، أرقام الرخص و السجلات و الممتلكات، أرقام الحسابات البنكية، بكاقات الإئتمان، الصور الثابتة أو المتحركة للمستخدم، و غيرها من البيانات ذات الطابع الشخصي. [1]

كما و حسب الاطار القانون الأروبي المذكور في(GDPR) فإن البيانات الشخصية تعتبر أي معلومة تبيح تمييز شخص طبيعي سواءا عبر اسم واضح أو رقم تعريفي أو من خلال ربط عوامل مثل بيانات الموقعأو معرفات الشبكة، تشمل أيضا خصائصه الجسدية مثل شكله الخارجي ، و الوراثي مثل جيناته و النفسية مثل حالته النفسية و العقلية و الاقتصادية و الثقافية، حتى انتماءاته الاجتماعية مثل علاقاته، يمكن أن تكون كذلك إشارة إلى موقعه الجغرافي أو بنيته الاقتصادية وة الاجتماعية التي تعكس هويته. [2]

كذلك تعرف البيانات الشخصية وفقا للقانون المصري بأنها تلك البيانات المتعلقة بشخص طبيعي يمكن تمييزه بصرف النظر عن إذا كانت هذه البيانات مباشرة أو غير مباشرة(3)، تشمل هذه البيانات أيضا الخصائص التي تحدد هوية الفرد بما في ذلك الصفات البدنية، الوراثية، الاقتصادية،...الخ، أو أي إشارة أخرى تتيح التعرف على الشخص. [3]

ثانيا: أنواع البيانات الشخصية:

الاتجاه الأول: اتجاه الناحية الرقمية التكنولوجية:

---

[1]- أنظر: هيئة الاتصالات و الفضاءات التقنية CST، مركز المعرفة الرقمية البيانات الشخصية تاريخ التصفح2025/05/09 ،الرابط: https://www.cst.gov.sa/ar/media-center

[2]- أنظر: محمد حسن و عماد مكاوي، الخصوصية الرقمية في القانون الدولي و المواثيق الدولية، مجلة البحوث و الدراسات الإعلامية، العدد22، 2022 ، ص 7

[3]- نفس المرجع، ص 8

البيانات الطوعية: وتشمل المعلومات التي يقدمها الفرد بإرادته المحضة عبر منصات رقمية مثل الاسم الذي يرفقه في حسابات الانترنت، الرقم التعريفي الذي تتم مشاركته في التطبيقات الالكترونية، او رقم الهوية الذي يدخل لإجراء خدمات رقمية.

البيانات المرصودة: يتضمن هذا النوع تلك المعلومات التي يتم جمعها بصفة تلقائية من خلال من خلال الأنظمة التكنولوجية، على سبيل المثال: بيانات الموقع الجغرافي المستقات من أجهزة الملاحة، عناوين (IP) التي تسجل اثناء تصفح الانترنت او السجلات الاتصال الالكتروني التي توثق نشاط الفرد في البيئة الرقمية.

البيانات الاستدلالية: تضم المعلومات المستنتجة من تحليل البيانات الرقمية كاستنتاج سلوكيات الفرد بناءا على تفاعلاته عبر الشبكات، تحديد اهتماماته من خلال بيانات تصفحه او استنتاج خصائصه الشخصية من خلال أنماط استخدامه للتطبيقات الالكترونية [1]

الاتجاه الثاني: الاتجاه الاجتماعي في تصنيف البيانات الشخصية

يرى هذا الاتجاه أن تصنيف البيانات الشخصية يجب أن ينطلق من طبيعة البيانات المرتبطة بهوية الفرد الاجتماعية والسياقية، سواء كانت قابلة لتحديد هوية الشخص بشكل مباشر أو غير مباشر، وذلك وفقًا لما يظهر من تفاعله داخل الفضاء الرقمي أو خارجه. ويُعتمد هذا التصنيف في عدد من الدراسات الحديثة التي تركز على أثر البيانات في الحياة الاجتماعية والخصوصية الفردية.

ويُعتبر من البيانات الشخصية وفقًا لهذا التصنيف كل من:

1-الاسم الكامل، والعنوان البريدي، والبريد الإلكتروني، ورقم الحماية الاجتماعية، ورقم جواز السفر، ورقم رخصة القيادة، وأرقام بطاقات الائتمان، وتاريخ الميلاد، ورقم الهاتف، وكافة البيانات التعريفية التي تُستخدم لتحديد هوية الفرد بشكل مباشر.

2-معلومات الجهاز، مثل رقم التعريف الخاص بالجهاز، تفاصيل الدخول، عنوان الـ IP، نوع المتصفح، أو نظام التشغيل، وغيرها من البيانات التقنية التي تُستخدم لتحديد هوية المستخدم عند ولوجه إلى الإنترنت.

3-بيانات الموقع الجغرافي، مثل عنوان السكن أو محل الإقامة، أو مكان العمل، أو أي موقع يرتبط بنشاط الفرد أو وجوده المكاني في الفضاء العام أو الخاص.

[1]- أنظر: نفس المرجع، ص 11

4-البيانات المدنية، وتشمل شهادة الميلاد، السن، تاريخ ومحل الميلاد، الحالة الاجتماعية، وكل ما يُستخرج من الوثائق الرسمية كجواز السفر أو رقم التأمين الاجتماعي.

5-الانتماءات والصفات الشخصية، مثل الدين، الجنس، الانتماء السياسي، أو الأصل العرقي، وغيرها من الخصائص التي تُستخدم لتصنيف الأشخاص اجتماعيًا أو ثقافيًا.

6-الوسائط الرقمية، كصور ومقاطع الفيديو التي يظهر فيها الفرد، أو أنماط التفاعل الخاصة به على منصات التواصل الاجتماعي، سواء تعلق الأمر بالبيانات المنشورة أو التعليقات أو الرسائل الخاصة.

ويؤخذ على هذا الاتجاه أنه يخلط أحيانًا بين البيانات الشخصية ذات الطابع التعريفي المباشر وتلك التي لا تُعرّف بالشكل المباشر ولكنها تُستخدم لبناء ملف شخصي للفرد أو لتوجيه الإعلانات أو القرارات الآلية نحوه[1]

الفرع الثالث: العلاقة بين الحق في الخصوصية الرقمية وبقية الحقوق الرقمية

تمثل الخصوصية الرقمية إحدى الركائز الأساسية للحقوق الرقمية، إذ يتوقف عليها التمتع الآمن بباقي الحقوق كالحق في حرية التعبير والأمن المعلوماتي. فعندما تُنتهك الخصوصية، تُهدّد تلقائيًا بقية الحقوق المرتبطة بها. لذلك، فإن حماية الخصوصية تُعد شرطًا جوهريًا لضمان بيئة رقمية تحترم الكرامة الإنسانية.

أولا: علاقته مع حق في حرية التعبير

يوجد توازن و ترابط دقيق بين كل من الخصوصية و حرية التعبير، خاصة اذا ما تعلق الامر ب النقد السياسي او الشخصيات العامة، حيث يطرح الجدل حول حدود هذا التوازن في ظل الفضاء الرقمي المفتوح، فالحق في التعبير لا يجب ان يستخدم كذريعة لانتهاك الخصوصية الاخرين ، خاصة حين يستعمل الإفصاح على الحياة الخاصة في غير محله، او حين يتحول الى وسيلة تهدف للتشهير او الحاق الضرر المعنوي و هو ما أكده بعض الباحثين في البيئة الرقمية مشددين على ان حرية التعبير لا تعني غياب ظوابط بل تتطلب مسؤولية قانونية عند التعرض لحياة الاخرين[2]

[1]- أنظر نفس المرجع،ص 11

[2]- انظر: احمد الشهري، "حرية التعبير و حدودها القانونية في البيئة الرقمية"، المجلة القانونية الجزائرية، العدد 44،2022،ص93

ثانيا علاقته مع الحق في أمن المعلومات

تتجسد العلاقة الوثيقة بين الخصوصية الرقمية و امن المعلومات في ان حماية البيانات الشخصية و تامينها ضد أي اختراق او تلاعب يعتبر من الشروط الأساسية و الجوهرية لضمان ممارسة خصوصية رقمية فعالة و مستدامة، فعندما يتم تعزيز امن البيانات من خلال تطبيق تقنيات التشفير المتقدمة، و وضع ضوابط صارمة للوصول الى المعلومات ،و تطوير اليات حماية قوية، يصبح من الممكن تعزيز حماية الخصوصية الرقمية بشكل كبير،فالامن السبراني يشكل الدرع الواقي الحامي للبيانات الشخصية من الانتهاكات ، مما يتيح للافراد التحكم في معلوماتهم الخاصة و و الحفاظ على سريتها كما انه و في غياب التدابير الأمنية الملائمة او ضعفها يعرض البيانات الشخصية لمخاطر عديدة، مما يتيح المجال للانتهاكات الخطيرة التي لا تقتصر على الخصوصية الرقمية فحسب، بل تمتد الى تهديد الحقوق الرقمية للاخرين فعلى سبيل المثال، قد يؤدي اختراق البيانات الى الكشف عن معلومات حساسة مثل توجهات الفكرية او المواقف السياسية او حتى التفاصيل المتعلقة بالحالة الصحية للافراد و هي معلومات يمكن ان تستخدم ضدهم بعدة طرق، كالابتزاز و التمييز و خضوعهم للاستهداف اللامشروع، بناءا على ذلك، يؤكد الكثير من الخبراء و الفقهاء في مجال القانون الرقمي ان تحقيق الخصوصية الرقمية لا يمكن ان يكون فعالا او مستداما دون وجود بنية تحتية رقمية امنة و أنظمة معلومات محمية بمعايير امنية عالية،تضمن الحفاظ على سلامة البيانات و سريتها[1]

ثالثا: الخصوصية كأساس للثقة الرقمية

تعتبر الخصوصية الرقمية العامل الأساسي لبناء الثقة بين المستخدم و الخدمات الرقمية فالثقة لاتتحقق فقط من خلال جودة الخدمة، بل تعتمد بشكل رئيسي على مدى احترام مقدم الخدمة لسرية البيانات المستخدم، و بالتالي فان نقص الشفافية في جمع البيانات و معالجتها يفقد المستخدم ثقته و هذا م اقد يدفعه للتوقف عن استخدام المنصة ،و تشير الباحثة هيلين نيستباوم الى ان الخصوصية ترتبط بسياقات محددة و أي انتهاك لهذه السياقات يضعف ثقة المستخدم و يهدد استقرار التفاعلات الاجتماعية.[2]

المطلب الثالث: الحق في النسيان الرقمي

شهد العصر الرقمي انفجارًا في حجم المعلومات الشخصية على الإنترنت، مما فرض الحاجة لآليات قانونية تضمن للأفراد التحكم في بياناتهم. ومن هذا المنطلق نشأ الحق في النسيان الرقمي، كأداة

[1]- انظر بلال جعفر، الامن السبراني و حماية البيانات الشخصية،دار الخلدونية، الجزائر،2020،ص47
[2]- أنظر: مرجع سابق،ص 11

لحماية الخصوصية والسمعة في الفضاء الرقمي، خاصة بعد انقضاء الحاجة القانونية أو الاجتماعية لهذه البيانات. ويتجلى هذا الحق بوضوح في التشريعات الأوروبية، خصوصًا بعد قضيةGoogle Spain .

الفرع الأول: تعريف الحق في النسيان الرقمي

هنالك من عرف الحق في النسيان بانه حق الشخص في السيطرة والتحكم في اي معلومة ذات طابع شخصي تخصه وفقا لهذا التعريف فان الفرد له الحق في ان يحتفظ طوال حياته بالسيطرة على ذكرياته الرقمية والتصرف فيها في اي وقت يريده والقيام بمحوها جزئيا او كليا متى راغب في ذلك وهذا التعريف تبنته اللجنة الوطنية للمعلوماتية في فرنسا حيث عرفت الحق في الدخول في طي النسيان الرقمي بانه الحق الذي يخول صاحبه مكانه السيطرة من حيث الزمان على بياناته الشخصية رؤية الحصول على حذفها او محوها عندما يرغب في ذلك[1].

في حين فقيه اخر ان الحق في النسيان هو حق يخور للشخص الطبيعي او الاعتباري مكانه محو معلومة تخصه او طلب التوقف عن نشرها بعد مرور فتره زمنية معينة.

هذا الفقيه والسعي في مجال الحق في النسيان ليجعل منه حق للأشخاص الاعتبارية كذلك اذ من خلاله يمكنهم كما للأشخاص الطبيعية حماية شخصيتهم الرقمية وذلك بالاعتراض على معالجه بياناتهم وطلب تعديلها او تصحيحها او تحديثها او منع الوصول اليها وكذا امكانيه المطالبة بمحوها وحذفها نهائيا.[2]

والملاحظ ان التعريف الموسع للحق في النسيان الرقمي يتوافق مع طبيعة البناء الهيكلي والفني لشبكه الانترنت فمستخدم الانترنت يفقد السيطرة على معلوماته الشخصية بمجرد نشرها ومن ثم تنتقل من موقع الى اخر ومن شخص الى اخر وقد تصبح هذه المعلومة قديمة وقد تكون في الاصل غير صحيحه لأنها منشوره من قبل الغير وهنا يكون تحت تصرف الشخص المعني كافة الوسائل القانونية التي تسمح له بحمايه شخصيته وهويته على شبكه الانترنت.

فان كان المحو النهائي للمعلومات شبه مستحيل فيكون في الاعتراض على المعالجة او طلب التصحيح او التحديث ما يمكن من خلاله تحقيق الحماية لصاحب المعلومة المتضرر او على الاقل ما يخفف من حجم الاضرار التي اصابتها.

[1]- بوخلوط الزين،الحق في النسيان الرقمي، مجلة المفكر،جامعة برج باجي مختار، العدد 14،ص551
[2]- بوخلوط الزين،الحق في النسيان الرقمي، مجلة المفكر،جامعة برج باجي مختار، العدد 14،ص551

ومن هذه التعاريف يمكن القول انه اذا كان الحق في الدخول في طي النسيان في صورته العامة يعني حق الفرض في بقاء ماضيه محاطا بسياج من الكتمان وعدم خروجه بعد مرور فتره زمنيه معينه الى العلن فان المقصود به في العالم الرقمي حق الفرد في الحصول على موافقته بشكل صريح وواضح عند البدء في جمع المعلومات الخاصة به وان يشرح له كيف تخزن ومده تخزينها والغاية من ذلك والحق في مسح المعلومات الشخصية التي تبقى عالقة في مختلف المواقع عبر شبكه الانترنت ويصعب عليه محوها بمفردها والتي من شانها ان تشكل انتهاكا لخصوصيته وتتسبب له في اضرار مادية ومعنوية.[1]

الفرع الثاني: الأساس القانوني للحق في النسيان

يرجع الاعتراف القانوني بالحق في النسيان إلى قضية محكمة العدل الأوروبية في 2014، حيث ألزمت المحكمة شركة Google بحذف روابط تؤدي إلى معلومات قديمة عن مواطن إسباني، معتبرة أن له حقًا في عدم ظهور بياناته الشخصية في نتائج البحث، متى فقدت هذه البيانات غرضها المشروع أو أصبحت مضرة1[2] .

ثم تم تقنين هذا الحق رسميًا في اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، التي دخلت حيز التنفيذ في عام 2018، وتنص المادة 17 منها على "الحق في المحو"، والذي يُمنح للمواطنين الأوروبيين لطلب حذف بياناتهم من قبل الهيئات أو الشركات التي تعالجها، بشرط انتفاء الحاجة إليها أو وجود ضرر2.

ويعد هذا الحق كحق في تقرير المصير المعلوماتي، الذي يمكن الأفراد من التحكم في مصير بياناتهم وهويتهم الرقمية[3] .

الفرع الثاني: تحديات الحق في النسيان وحدوده القانونية

رغم أهمية الحق في النسيان الرقمي كوسيلة لحماية الخصوصية الرقمية، إلا أن تطبيقه يواجه جملة من التحديات، القانونية والتقنية والثقافية، نستعرض هذه التحديات، ثم نقترح آليات عملية للتفعيل.

أولا: التحديات القانونية

---

[1]- انظر:بوخلوط الزين،الحق في النسيان الرقمي، مجلة المفكر،جامعة برج باجي مختار، العدد 14،ص551

[2]- موقع محكمة العدل الأوروبية: الرابط تاريخ التصفح 2025/06/26
https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=FR

[3]- انظر:اللائحة العامة لحماية البيانات، المادة 17

يعد التوتر بين الحق في النسيان الرقمي وحرية التعبير من أبرز التحديات القانونية المطروحة على الساحة الحقوقية. ففي الوقت الذي يمنح فيه الحق في النسيان الأفراد إمكانية حذف أو حجب بياناتهم القديمة من محركات البحث أو المواقع الإلكترونية، فإن ذلك قد يُعد تقييدًا غير مبرر لحق الجمهور في الوصول إلى المعلومة، خاصة إذا تعلّق الأمر بأحداث تاريخية أو قضايا ذات طابع عام.

فإن حماية سمعة الأفراد وكرامتهم الرقمية يجب ألا تأتي على حساب طمس الحقائق أو فرض رقابة ناعمة باسم الخصوصية. لذا فإن صياغة هذا الحق يتطلب إدراكًا دقيقًا للحدود المشروعة بين الحياة الخاصة وحرية التعبير، والتمييز بين المعلومات ذات الطابع الشخصي، وتلك التي تخدم المصلحة العامة أو التاريخ المشترك.[1]

ثانيا: التحديات التقنية والعملية

الحق في النسيان يواجه أيضًا تحديات تقنية تجعل تنفيذه شبه مستحيل في بعض الحالات. فبمجرد نشر البيانات على شبكة الإنترنت، تصبح هذه المعلومات جزءًا من منظومة أرشفة عالمية، وتُخزن على سيرفرات متعددة موزعة عبر دول مختلفة. حتى وإن تم حذف المعلومات من الموقع الأصلي، فإنها قد تظل محفوظة في ذاكرة التخزين المؤقت، أو لدى طرف ثالث قام بإعادة نشرها.

كما أن نسبة كبيرة من المستخدمين لا يعرفون بوجود هذا الحق أصلًا، أو يخلطون بينه وبين مفاهيم أخرى مثل "الخصوصية" أو "الحق في الحذف المؤقت". هذا الجهل القانوني يضعف من فاعلية أي نص تشريعي، لأن ممارسة الحقوق الرقمية ترتبط بالمعرفة بها أولًا. كما أن غياب قنوات واضحة لتقديم طلبات الحذف، وصعوبة التواصل مع الجهات المعنية (سواء الشركات التقنية أو الهيئات الوطنية)، يعمق من شعور المستخدم بالعجز إزاء بياناته الشخصية المنشورة على الإنترنت[2].

ثالثا: آليات مقترحة لتفعيل الحق في النسيان الرقمي

ينبغي أن تتبنى الدول نصوصا قانونية صريحة تضمن الحق في النسيان الرقمي ضمن قوانين حماية البيانات، مع تحديد نطاقه، وشروطه، وإجراءاته، والجهات المختصة بتنفيذه. كما يجب استلهام

[1]- أنس *الحجاجي*، الحق في النسيان الرقمي: محاولة لفهم المفهوم وتحديات إدماجه في النظام *القانوني المغربي*، مجلة الحقوق، المغرب، 2021.

[2]- انظر أنس الحجاجي، *الحق في النسيان الرقمي: محاولة لفهم المفهوم وتحديات إدماجه في النظام القانوني المغربي*، مجلة الحقوق، المغرب، 2021.

التجربة الأوروبية، خصوصًا المادة 17 من اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، والتي نصت على "الحق في المحو" كحق قابل للتطبيق في حالات محددة[1] .

كما يتعين إنشاء هيئات وطنية مستقلة لحماية البيانات الشخصية تكون مسؤولة عن تلقي شكاوى الأفراد، والتحقيق فيها، وإصدار قرارات ملزمة تجاه المنصات الرقمية ومحركات البحث، وتوفير نماذج موحدة لطلبات الحذف، مع ضمان حق الأفراد في الطعن القضائي ضد قرارات الرفض.

و بما أن الفضاء الرقمي لا يعترف بالحدود الجغرافية، فإن تفعيل الحق في النسيان الرقمي يحتاج إلى تعاون دولي، من خلال اتفاقيات لحماية البيانات بين الدول، وتبادل المساعدة في تنفيذ قرارات الحذف الصادرة عن جهة قضائية في دولة ما على مزودي خدمة موجودين في دولة أخرى.

إن نجاح أي تشريع متعلق بالحق في النسيان يتوقف على مدى وعي المواطنين بأهمية هذا الحق، وطرق ممارسته. لذا، ينبغي إطلاق حملات توعية وطنية على مستوى الإعلام والمؤسسات التعليمية لتعزيز ثقافة الحقوق الرقمية، وشرح سبل الحماية القانونية في البيئة الإلكترونية.

المطلب الرابع: الامن السبراني من اجراء وقائي لضمان الحقوق الرقمية الى حق قائم بذاته

يشهد العالم تطورًا متسارعًا في مجال التكنولوجيا الرقمية، ما جعل الفضاء السيبراني عنصرًا أساسيًا في مختلف مجالات الحياة. ومع هذا التوسع، ظهرت تهديدات إلكترونية متزايدة طالت خصوصية الأفراد وأمن بياناتهم وسلامة الأنظمة الرقمية. في هذا السياق، برز الأمن السيبراني كوسيلة لحماية الحقوق الرقمية وضمان ممارستها في بيئة آمنة. وقد تطور دوره تدريجيًا من مجرد إجراء وقائي إلى ضرورة قانونية لحماية المستخدمين من المخاطر الرقمية. وأمام اتساع نطاق استخدام التكنولوجيا، أضحى الأمن السيبراني يُنظر إليه كحق رقمي قائم بذاته لا غنى عنه في البيئة الرقمية المعاصرة.

الفرع الأول: المفهوم العام للأمن السبراني:

تم تعريف الامن السيبراني بانه مجموع الوسائل التقنية والتنظيمية والبشرية التي تهدف الى حماية الفضاء الرقمي من الهجمات الإلكترونية والحفاظ على سريه وسلامه وتوفير المعلومات ونظم الاتصالات ويعد هذا المفهوم حديثا نسبيا اذ ابرز نتيجة توسع الهائل في استخدام تقنيات الاتصال والمعلومات وما رافقها من تطور في الهجمات والتهديدات الرقمية

كما يأخذ هذا المفهوم بعدا شموليا فلا يقتصر فقط على حماية البنى التحتية الرقمية بل يشمل ايضا حماية حقوق الافراد في في بيئة الانترنت لاسيما حقهم في الخصوصية الرقمية وعدم تعريضهم

[1]- انظر:اللائحة العامة لحماية البيانات، المادة 17

للابتزاز او المراقبة غير المشروعة وعليه فان الامن السيبراني لا يجب ان يتم فهمه او تداوله على انه اجراء وقائي فقط بل لك حق من حقوق الانسان في العالم الرقمي اذ يمكن الافراد من التفاعل والمشاركة بحريه وامان داخل البيئة الإلكترونية. [1]

يعرف الامن السيبراني كذلك بانه تامين كل الفضاء السيبراني الموجود والمترابط شبكيا من البنية التحتية لتقنيه المعلومات والتي تشمل الانترنت وشبكه الاتصال وانظمه الحاسب الالي والأجهزة المتصلة بالأنترنت الى جانب المعالجات واجهزه التحكم المرتبطة بها.

كما يعرف كذلك على انه القدرة على صد الخطر عن الفضاء السيبراني وحمايته من الهجمات الإلكترونية التي من شانها استهداف انظمه المعلومات او السعي للوصول الى البيانات وتعديلها او تدميرها بشكل غير مشروع مع ضمان استمراريه الخدمة وسلامه المعلومات. [2]

يقصد بالأمن السيبراني ايضا انه مجموعه الاطر التنظيمية والقانونية والتقنية التي تسعى الى حماية الانترنت والفضاء السيبراني من خطر التهديدات بما فيه امن الشبكة والمعلومات وحظر استغلالها ويهدف الى تحقيق سلامه البنى التحتية الوطنية وحمايه المعلومات الشخصية.

حسب الاتحاد الدولي للاتصالات يقصد بالأمن السيبراني انه تلك المجموعة المتكاملة من الادوات والسياسات والمفاهيم والممارسات الفنية والتنظيمية مثل اداره المخاطر والتدريب والتقنيات التي تسعى الى حماية الفضاء الرقم والممتلكات والمستخدمين والمؤسسات من التهديدات والمخاطر الرقمية. [3]

اما وكاله الامن السيبراني وامن البنية التحتية الأمريكية فتعرف الامن السيبراني على انه مجموعه الجهود التي تسعى الى حماية الشبكات والأجهزة والبيانات من الوصول او الاستخدام لا مشروع مع التأكيد على الحفاظ على سريه المعلومات وسلامتها وتوفرها عند الحاجة. [4]

الفرع الثاني: طبيعة الحق في الامن السبراني

أولا: الطابع الفردي والجماعي:

فالحق في الامن السيبراني يتميز بطبيعة مزدوجة حيث يجمع بين البعد الفردي والبعد الجماعي في نفس الوقت فعل المستوى الفردي يعد هذا الحق ضمانا لكل مستخدم لحماية معطياته الرقمية

[1]- جعفر بلال، مرجع سابق، ص 27
[2]- اسماء حاتم، الامن السيبراني وامن المعلومات، جامعه طيبه، قسم علوم الحاسب والمعلومات، صفحه 22
[3]- نفس المرجع، ص 22
[4]- الامن السيبراني، مفهومه وتاريخه موقع قناة الجزيرة، تاريخ التصفح: 2025/05/11:
https://www.aljazeera.net/encyclopedia/2024/9/19/

ومعلوماته الخاصة من التهديدات والاخطار السيبرانيه كالتجسس وسرقه البيانات واختراق الأجهزة كما يسمح هذا البعد للفرد بممارسه انشطته الرقمية في بيئة امنة وخالية من التهديدات مما يعزز الثقة في استخدام الوسائل التكنولوجية الحديثة.

اما على المستوى الجماعي فيعتبر الامن السيبراني من الأعمدة الأساسية للحفاظ على امن الدولة والمجتمع خاصه امام تطور الهجمات الإلكترونية التي تسعى للوصول واستهداف البنى التحتية الحساسة مثل قطاعات الدفاعية والمالية والطبية وعليه فان حماية الفضاء السيبراني لا تمثل فقط مسؤوليه فرديه بل هي كذلك التزام جماعي يتطلب التنسيق بين الافراد والمؤسسات والدولة لضمان استقراره. [1]

وبالتالي فان الطبيعة المزدوجة التي يمتاز بها هذا الحق في الامن السيبراني لا يعكس فقط مستوياته المختلفة (الفردي والجماعي) بل يعبر ايضا عن ترابط مسؤوليات متعددة بداية من الفرد الذي عليه التحلي بالوعي الرقمي مرورا بالمؤسسات التي يقع على عاتقها تامين البنيات التحتية الخاصة بها وصولا الى الدول التي من شانها تحمل مسؤوليه وضع استراتيجيات وطنيه شامله ومدروسة لمواجهه التهديدات السيبرانيه. [2]

ثانيا الطبيعة الديناميكية

يتصف الحق في الامن السيبراني بطبيعة ديناميكية تجعل منه حقا قابلا للتطور المستمر اذ يرتبط بشكل وثيق مع التغيرات الطارئة في البيئة التكنولوجية وتحدياتها المتجددة مع تزايد الاعتماد على الوسائل الرقمية ظهرت تهديدات سيبرانيه حديثه كالهجمات المعقدة على تقنيه الذكاء الاصطناعي او استغلال نقاط الضعف اجهزه الانترنت ما يجعل من الضروري اعاده النظر في السياسات الأمنية بشكل دوري ضمانا لقدرتها على الاستجابة السريعة والفعالة لهذه المخاطر المتنامية ومن هذا المنظور لا يمكن التعامل مع الامن السيبراني كمفهوم جامد وتقليدي بل كحق مرن قابل للتجدد ومتطلب لليقظة الدائمة ومواكبه مستمرة للتطورات التقنية. [3]

ثالثا: حق تمكيني

يؤدي الامن السيبراني دورا تمكينيا مهما اذ انه يوفر بيئة ملائمه لممارسه الحقوق الرقمية المختلفة فلا يمكن ضمان الحق في الخصوصية او حريه التعبير مثلا دون وجود تدابير امنيه تحول وتسريب المعلومات او اعتراضها فالفرض في البيئة الرقمية لن يتمكن من اداء دوره المدني او

[1]- اللجنة الأوروبية للحقوق الرقمية: دليل الامن السيبراني وحقوق الانسان، بروكسل، 2020، ص 5
[2]- نفس المرجع، ص 5
[3]- نفس المرجع، ص 6

المشاركة في النقاشات إذا شعر ان بياناته معرضه للاختراق او ان يخضع لمراقبه تحركاته دون اي مبرر قانوني.

الفرع الثالث: أبعاد الامن السبراني في مختلف المجالات

أولا: البعد التقني:

ويركز هذا المكون على استعمال الادوات والتقنيات المتقدمة لحماية البيانات والمعلومات من التهديدات السيبرانية مثل القرصنة او التسريب ويتضمن ذلك تطبيق تقنيات امنيه كجدران حماية وانظمه التشفير المتطورة وبرمجيات مكافحه الفيروسات اضافه الى اعتماد سياسات منتظمة للنسخ الاحتياطي لضمان استمراريه البيانات وسلامتها كما يتطلب هذا المكون التحديث المستمر والدوري للبرمجيات والتطبيقات حيث تستغل معظم الهجمات السيبرانيه الثغرات الأمنية التي لم يتم اكتشافها او معالجتها في الأنظمة القديمة. [1]

ثانيا: البعد الادراكي والثقافي:

يعمل هذا البعد على رفع الوعي لدى المستخدمين بالمخاطر الرقمية وطرق الحماية منها فالكثير من الثغرات الأمنية لا تكون نتيجة اسباب تقنيه فقط بل ايضا لها علاقة بسلوكيات البشرية الخاطئة على سبيل المثال استخدام كلمات مرور ضعيفة او النقر على روابط مجهولة وعليه فان التربية الرقمية والتكوين المستمر يعتبران عنصرين اساسيين لبناء امن السيبراني فعال. [2]

ثالثا: البعد الاجتماعي:

يتمثل البعد الاجتماعي في التأثير الامن السيبراني على مستوى الثقة الرقمية التي تربط بين المستخدمين ومقدمي الخدمات الرقمية اذ عندما يشعر الافراد بان بياناتهم الشخصية محميه ومؤمن عليها يزداد اطمئنانهم واستعدادهم للتفاعل مع المنصات الرقمية واجراء المعاملات الإلكترونية بثقة مما يعزز من عمليه التحول الرقمي ويسهم في تعميقه داخل المجتمع.

رابعا: البعد القانوني

يتطلب الامن السيبراني اقامه إطار قانوني وتنظيمي متكامل يتماشى مع التطورات والتحولات الرقمية المتسارعة حيث لا يقتصر هذا البعد على مجرد اصدار تشريعات وسن قوانين بل يمتد الى انشاء

[1]- الاتحاد الدولي للاتصالات فهم الامن السيبراني في المجتمع الرقمي 2019 ص 13، متاح على الموقع: /https://www.itu.int/itu-d/sites/cybersecurity/ar

[2]- البنك الدولي الحوكمة الرقمية والتنمية، واشنطن، 2022، ص 89

مؤسسه متخصصة مكلفه بالحرص على تنفيذ وتطبيق هذه القوانين الى جانب توفير اليات فعاله متخصصة في تنفيذ والرقابة المستمرة ففي غياب هذه الاطر القانونية المتينة يصبح المجال مفتوح امام الانتهاكات والتهديدات السيبرانيه مما يؤثر على قدره الفرد على حماية حقوقه الرقمية او متابعه الجهات المعتدية قانونيا. [1]

[1]- الامم المتحدة: الجمعية العامة، تعزيز الامن السيبراني وحماية حقوق الانسان، وثيقة A/76/136 2021 الفقرة 18، متاح على الموقع: https://digitallibrary.un.org/?ln=ar

الفصل الثاني:

الإطار القانوني للحقوق الرقمية على المستوى الدولي

الفصل الثاني: الإطار القانوني للحقوق الرقمية على المستوى الدولي

مع تطور الوسائط الرقمية وازدياد الاعتماد على الإنترنت في مختلف مجالات الحياة، برزت الحاجة إلى حماية حقوق الإنسان في الفضاء الرقمي، باعتبارها امتدادًا طبيعياً للحقوق والحريات الأساسية. وقد أدى هذا التحول إلى بروز تحديات قانونية جديدة، تتطلب تدخلًا تشريعيًا دوليًا منسقًا يواكب التغيرات التقنية ويضمن عدم انتهاك كرامة الأفراد وخصوصياتهم.

ولأن طبيعة الفضاء الرقمي عابرة للحدود، فقد أصبح من الضروري وضع إطار قانوني دولي ينظّم الحقوق الرقمية، ويؤسس لمبادئ واضحة تحمي المستخدمين من الممارسات التعسفية، سواء من قبل الدول أو الشركات أو الفاعلين غير الحكوميين. ومن هذا المنطلق، تبلورت العديد من الاتفاقيات والمواثيق الدولية التي تسعى إلى إرساء قواعد قانونية مشتركة، كما ظهرت جهود متعددة الأطراف لتفعيل تلك المبادئ في الواقع العملي، خصوصًا في ظل التحديات التي تفرضها المراقبة الإلكترونية، والهجمات السيبرانية، والتمييز الخوارزمي، وغيرها من الظواهر المرتبطة بالتحول الرقمي.

وسيتناول هذا الفصل دراسة الإطار القانوني الدولي الذي يُنظّم الحقوق الرقمية، من خلال مبحثين أساسيين:

المبحث الأول :الاتفاقيات واللوائح الدولية ذات الصلة بحماية الحقوق الرقمية،

المبحث الثاني :الجهود الدولية المبذولة لحماية هذه الحقوق في ظل التحديات الراهنة.

المبحث الأول: الاتفاقيات واللوائح الدولية الدولية ذات الصلة

أدرك المجتمع الدولي مبكرًا أن التطور الرقمي يحمل في طياته إمكانات هائلة لتعزيز حقوق الإنسان، لكنه في الوقت ذاته يطرح مخاطر جديدة قد تهدد هذه الحقوق بطرق غير مسبوقة. وقد دفع هذا الإدراك إلى بروز اهتمام متزايد على المستوى الدولي بضرورة وضع أطر قانونية تحكم الفضاء الرقمي وتحمي المستخدمين من الانتهاكات التي قد يتعرضون لها أثناء تفاعلهم مع التكنولوجيا الحديثة.

فمع أن الكثير من الحقوق الرقمية تُعد امتدادًا لحقوق الإنسان التقليدية، فإن البيئة الرقمية تفرض تحديات نوعية، خاصة من حيث الخصوصية، حرية التعبير، حماية البيانات، والأمن السيبراني. وقد تنبّهت الأمم المتحدة، إلى جانب عدد من المنظمات الدولية والإقليمية، إلى هذا الواقع، فسعت إلى تضمين الحقوقالرقمية في الاتفاقيات العامة لحقوق الإنسان، كما عملت على إبرام اتفاقيات متخصصة ووضع لوائح تقنية وقانونية تُعنى بحماية الأفراد في البيئة الإلكترونية.

وعليه، يهدف هذا المبحث إلى استعراض أهم الاتفاقيات واللوائح الدولية التي ساهمت في بلورة الإطار القانوني للحقوق الرقمية، مع تسليط الضوء على مضامينها

المطلب الأول: الشرعة الدولية لحقوق الانسان

يشكل الإعلان العالمي لحقوق الإنسان والعهدان الدوليان الإطار المرجعي الأساسي لحماية حقوق الإنسان، بما في ذلك تلك الممارسة في الفضاء الرقمي. ومع تطور التكنولوجيا، أصبحت الحقوق الرقمية امتداداً طبيعياً لهذه المواثيق، خاصة فيما يتعلق بحرية التعبير، وحماية الخصوصية، والحق في الوصول إلى المعلومات. ورغم أن النصوص الأصلية لا تذكر التكنولوجيا صراحة، إلا أن مبادئها قابلة للتطبيق على البيئة الرقمية. لذا، فإن فهم هذه المرجعيات ضروري لضمان حماية فعالة للحقوق في العصر الرقمي.

الفرع الأول: استغراق مواد الإعلان العالمي لحقوق الإنسان للحقوق الرقمية

يعتبر الإعلان العالمي لحقوق الإنسان أول وثيقة عالمية وضعية تناولت حقوق الإنسان بصفة شاملة، وأحاطتها بجملة من الضمانات القضائية، وقد كان شاملا ويحوي على حقوق الإنسان بما فيه الكفاية، حيث يعد الوثيقة الحقوقية الأشهر في العصر الحديث، و قد صدر عن الجمعية العامة لمنظمة الأمم المتحدة في العاشر من ديسمبر1948 بعد الحرب العالمية الأولى التي قتل فيها أكثر من خمسة عشر مليون انسان، وبعد مشروع العصبة الأمم الذي فشل في منع وقوع الحرب العالمية الثانية ، التي ازهقت فيها أكثر من خمسين مليون نفس، و دمار مروع في المباني والممتلكات في أغلب مناطق العالم.

ان المتمعن في هذا النص الحقوقي الإعلان العالمي لحقوق الانسان يجد بأنه أسس لمعارف وحقائق ووقائع سياسية لمتعرف سابقا، ففي بنوده نجد أنه يوحي بتقدم كبير للبشرية في مجال الحقوق والحريات الفردية.

يحوي الإعلان ديباجة وثلاثين مادة، تحدد حقوق الإنسان وحرياته الأساسية التي تحق لجميع الرجال والنساء على حد سواء، في كل مكان في العالم دون أي تمييز، وهو أمر لم يكن معروفا في الأزمنة السابقة والعصور الدولية القديمة، التي كان أول ظهور لنظام دولي فيها هو قيام عصبة الأمم عام 1919 حيث وجد لأول مرة ما يعرف اليوم بالنظام الدولي والمجتمع الدولي بعدما كانت السياسات سابقا تقوم بين الدول ثنائيا بالعلاقات السياسية والمعاهدات وتبادل السفراء.

ان الشكل الذي صدر فيها لإعلان العالمي لحقوق الانسان يبعث على الشك فيما يخص القوة القانونية الإلزامية لنصوصه، فصدور الإعلان في شكل توصية جعلته كغيره من اللوائح الأخرى للجمعية العامة لمنظمة الأمم المتحدة التي لا ترتب التزامات على الدول، وهذا ما أكده المكلفون بإعداد، ولهذا اعتمدت الجمعية العامة لمنظمة الأمم المتحدة العهدين الدوليين، الأول خاص بالحقوق الاقتصادية و الاجتماعية و الثقافية، والثاني خاص بالحقوق السياسية و المدنية بقرارها رقم(2200) المؤرخ في1966/12/16 والبروتوكولين الاختياريين الملحقين بالعهد الدولي للحقوق السياسية والمدنية من أجل إضفاء الطبيعة الإلزامية للبنود الواردة في الإعلان.[1]

ومن خلال دراسة مواد الإعلان العالمي لحقوق الإنسان نجدها تستوعب الحقوق الرقمية باعتبارها جاءت في شكل واسع وصيغة مفتوحة حيث تعد المادة 19 من الإعلان العالمي لحقوق الإنسان (1948) المرجعية الدولية الأولى لحرية التعبير، حيث تنص على" *لكلِّ شخص حقُّ التمتُّع بحرّية الرأي والتعبير، ويشمل هذا الحقُّ حرّيته في اعتناق الآراء دون مضايقة، وفي التماس الأنباء والأفكار وتلقِّيها ونقلها إلى الآخرين، بأيَّة وسيلة ودونما اعتبار للحدود* ."وتمتاز هذه المادة بصياغتها العامة التي تجعلها قابلة للتطبيق حتى في ظل الوسائل التكنولوجيةالحديثة، رغم أنها لم تكن معروفة آنذاك.

إنّ عبارة" بأي وسيلة "الواردة في المادة 19 تُعدّ صيغة مفتوحة تتيح التوسع في مفهوم الوسائل لتشمل جميع التقنيات المعاصرة والمستقبلية، بما في ذلك الإنترنت، وتطبيقات الهواتف، ومنصات

[1]- انظر: لونيسي علي، دور الإعلان العالمي لحقوق الانسان في إقرار الضمانات القضائية لحقوق الانسان،مجلة الأستاذ الباحث للدراسات القانونية و السياسية ،المجلد 04، العدد 02،ص 2058-2059

الإعلام الرقمي. هذا التوسع هو ما جعل من المادة 19 مرجعًا قانونيًا يواكب التطور الرقمي ويؤسس لحق الإنسان في حرية التعبير داخل الفضاء السيبراني.[1]

حيث أصبح التعبير عن الرأي في العصر الرقمي لا ينحصر في الكلمة المطبوعة أو الصوت المسموع، بل اتخذ أشكالًا متعددة مثل:

- كتابة التدوينات والمقالات على المدونات الشخصية أو مواقع الرأي.

- مشاركة الفيديوهات على منصات مثل يوتيوب وتيك توك.

النشر والتغريد عبر منصات مثل تويتروفيسبوك.

تُمثل هذه الأشكال المعاصرة أدوات تمكّن الأفراد من التفاعل والمشاركة في النقاش العام، وهي امتداد طبيعي للحق التقليدي في حرية التعبير.

كما أصبحت الإنترنت أداة أساسية لممارسة حرية التعبير في المجتمعات المعاصرة، وبالتالي فإن حرمان الأفراد من الوصول إليه يعد شكلا من أشكال التقييد غير المباشر لهذا الحق. وقد أكدت العديد من التقارير الأممية أن حرية التعبير في العصر الرقمي لا يمكن فصلها عن الحق في الوصول إلى الإنترنت.

كما تنص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه" :لا يجوز تعريض أحد لتدخل *تعسفي* فيحياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات ."وقد جاءت هذه المادة لتُرسّخ مبدأ احترام الحياة الخاصة كأحد الحقوق الأساسية التي لا يجوز انتهاكها، سواء من قبل سلطات الدولة أو من قبل الأفراد أو الكيانات الخاصة. وإذا كان مفهوم الحياة الخاصة في السابق يقتصر على الفضاء المادي كالمسكن والمراسلات الورقية والعلاقات الأسرية، فإن التطورات التكنولوجية التي شهدها العالم خلال العقود الأخيرة قد فرضت واقعًا جديدًا، أصبحت فيه الحياة الخاصة تمتد إلى الفضاء الرقمي، حيث يتم تخزين البيانات الشخصية، وتبادل المراسلات، ومشاركة الصور، وتتبع السلوكيات الرقمية على نطاق واسع. إلا أن هذا التطور رافقه في المقابل بروز تهديدات غير مسبوقة تستهدف خصوصية الأفراد في هذا الفضاء الجديد، لعل أبرزها الاختراق الإلكتروني، وهو دخول غير مشروع إلى الحسابات الشخصية والبيانات الرقمية المخزنة للأفراد، بما يشكل انتهاكًا مباشرًا لحياتهم الخاصة. كما ظهرت ممارسات المراقبة الجماعية التي تقوم بها بعض الحكومات عبر برامج تجسسية واسعة

[1]- انظر: محمد عبد العزيز عبد المنعم، *حرية التعبير في العصر الرقمي: الضوابط والقيود في القانون الدولي*، المركز القومي للبحوث الجنائية والاجتماعية، القاهرة، 2017، ص. 88.

النطاق، مثل برنامج PRISM الأميركي، والتي تتيح رصد كميات هائلة من المعلومات الشخصية دون علم الأفراد أو موافقتهم. ومن جهة أخرى، برز خطر تتبع البيانات الشخصية من قبل شركات التكنولوجيا الكبرى، التي تجمع معلومات المستخدمين وتستخدمها لأغراض تجارية واستهداف إعلاني، غالبًا دون موافقة صريحة من أصحاب البيانات، وهو ما يُعد انتهاكًا واضحًا لخصوصيتهم الرقمية. وتفرض المادة 12 على الدول التزامات قانونية واضحة في مواجهة هذه التحديات، إذ لم يعد كافيًا الاكتفاء بالنصوص العامة، بل يجب سن تشريعات صريحة تضمن حماية البيانات الشخصية في البيئة الرقمية. ومن الأمثلة الرائدة في هذا السياق، اللائحة العامة لحماية البيانات (GDPR) التي اعتمدها الاتحاد الأوروبي، والتي تُعتبر نموذجًا متقدمًا لحماية خصوصية الأفراد، حيث تُمكنهم من التحكم في بياناتهم والاطلاع عليها، وطلب حذفها، والموافقة على استخدامها بشكل واضح. وكذلك الأمر بالنسبة لقانون خصوصية المستهلك في كاليفورنيا (CCPA) الذي يمنح الأفراد حق معرفة البيانات التي تُجمع عنهم، ورفض بيعها أو مشاركتها مع أطراف ثالثة. إن هذه التشريعات تعكس تحولًا جوهريًا في فهم الخصوصية، واعتبارها حقًا رقميًا أساسيًا لا يقل أهمية عن الحقوق التقليدية. وعليه، فإن أي إهمال في سن مثل هذه القوانين أو في تطبيقها، يُعد إخلالًا بالالتزامات التي تفرضها المادة 12 من الإعلان العالمي لحقوق الإنسان، مما يهدد الأساس الذي تقوم عليه حماية الكرامة الإنسانية في العصر الرقمي[1]

وتنص المادتان 26 و27 من الإعلان العالمي لحقوق الإنسان على أن لكل شخص الحق في التعليم والمشاركة الحرة في الحياة الثقافية للمجتمع، والاستفادة من الفنون والمساهمة في التقدم العلمي، وتؤكد المادة 26 أن التعليم يجب أن يكون مجانياً في مراحله الأساسية، وأن يُتاح التعليم الفني والمهني للجميع، مع ضمان تكافؤ الفرص في التعليم العالي تبعاً للكفاءة. ولا يقف التعليم عند التلقين، بل يجب أن يستهدف تطوير شخصية الإنسان وتعزيز احترام حقوق الإنسان والحريات الأساسية، وغرس قيم التسامح والتفاهم بين الشعوب والثقافات. أما المادة 27، فقد نصّت على حق كل فرد في المشاركة في الحياة الثقافية، والتمتع بالفنون، والمساهمة في النشاط العلمي، إلى جانب الحق في حماية حقوقه الأدبية والمادية الناتجة عن إنتاجاته الفكرية أو الفنية[2]

وفي ضوء التحول الرقمي الذي يشهده العالم، أصبح هذان الحقّان – في التعليم والمشاركة الثقافية – مرتبطين ارتباطًا وثيقًا **بالبيئة الرقمية** .فالحق في التعليم في العصر الحديث لا يكتمل دون**القدرة على الوصول إلى الإنترنت**، باعتبارها مصدراً أساسياً للمعرفة والتعلُّم، ومنصة لفرص التعليم

[1]- انظر: هالة أبو الحسن، القانون والتكنولوجيا: حماية البيانات الشخصية في البيئة الرقمية، دار النهضة العربية، القاهرة، 2021، ص. 122–126.

[2]- انظر خالد العربي، حقوق الإنسان في المواثيق الدولية والواقع العربي، دار الشروق، القاهرة، 2018، ص. 174

المفتوح والتعليم عن بُعد. كما أن استخدام **الأدوات التكنولوجية**واكتساب **المهارات الرقمية**أصبح شرطاً ضرورياً للاندماج في المنظومة التعليمية، سواء فيما يتعلق باستخدام المنصات التعليمية أو التواصل مع المعلمين أو إجراء الأبحاث. وبالتالي، فإن **التمييز الرقمي** وعدم توفير البنية التحتية المناسبة يُعد نوعاً من الإقصاء عن الحق في التعليم.[1]

وفي السياق نفسه، فإن **المشاركة الثقافية** لم تعد تقتصر على الحضور الفعلي في المسارح أو المعارض أو المكتبات، بل اتسعت لتشمل الوصول إلى **المكتبات الرقمية**، ومتابعة **العروض الفنية والبصرية** عبر الإنترنت، والاستماع إلى **الموسيقى والبودكاست**، والمشاركة في إنتاج المحتوى الثقافي من خلال منصات مثل **يوتيوب وتيك توك** .بل وأصبح التفاعل الثقافي متعدد الاتجاهات، حيث لم يعد الفرد مجرد متلقٍّ، بل منتجاً ومساهماً في إثراء الثقافة الرقمية.

حيث ان احترام ما ورد في المادتين 26 و27 في العصر الرقمي يقتضي من الدول العمل على **ضمان النفاذ المفتوح والعادل إلى الإنترنت**، وتوفير **البنية التحتية الرقمية**، وضمان **التعليم الرقمي المتاح**، و**حماية الإنتاج الثقافي الرقمي**، بما يكفل لكل فرد الحق في التعلم والمشاركة الثقافية على قدم المساواة، وفق ما تفرضه تطورات الواقع الرقمي.

الفرع الثاني: استغراق مواد العهد الدولي الخاص بالحقوق المدنية والسياسية للحقوق الرقمية

يعد العهد الدولي الخاص بالحقوق المدنية والسياسية من أهم الوثائق الدولية المعنية بتنظيم حقوق الإنسان على مستوى العالم، وهو بمثابة معاهدة متعددة الأطراف اعتمدتها الجمعية العامة للأمم المتحدة في 16 ديسمبر 1966، ودخلت حيّز التنفيذ في 23 مارس 1976. كما يعتبر العهد الدولي جزءً من الشرعة الدولية لحقوق الإنسان التي تشمل أيضاً العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، والإعلان العالمي لحقوق الإنسان.

العهد الدولي يلزم كافة الدول الأطراف الموقعة على هذه الاتفاقية الدولية احترام الحقوق المدنية والسياسية للأفراد، وتشمل الحق في الحياة، والحرية الدينية، وحرية التعبير، وحرية الإنسان، وحقوق التجمع والانتخاب، والتقاضي، والمحاكمة العادلة.

وتتولى لجنة حقوق الإنسان وهي هيئة مستقلة لمجلس حقوق الإنسان التابع للأمم المتحدة متابعة هذا العهد والتأكد من التزام الدول الأطراف الموقعة على هذه الاتفاقية الدولية بما جاء فيه من خلال آلية منتظمة لاستعراض تقارير الدول الأطراف بشأن إجراءاتها في تنفيذ واحترام الحقوق الواردة في العهد

[1]- انظر: نفس المرجع 2018، ص. 176.

الدولي. وتُكلف كافة الدول الأطراف في العهد نفسه تقديم تقرير أولي بعد سنة واحدة من التصديق عليه، كما وتطلب لجنة حقوق الإنسان تقريراً من الدولة نفسها، وهو إجراء يتم في الغالب كل أربع سنوات، حيث تجتمع اللجنة في المقر الأوروبي للأمم المتحدة بجنيف وتعقد ثلاث دورات سنوياً لتحقيق هذا الهدف.

يتكون العهد الدولي من ديباجة، وستة أجزاء تضم 53 مادة. ويقوم بداية على تأكيد الحقوق الإنسانية المدنية والسياسية العامة. ويتناول كل جزء مجموعة من الحقوق التي ينبغي احترامها، إذ يتناول الجزء الأول حق مختلف الشعوب في تقرير مصيرها، وأن تسعى لتحقيق أهدافها الخاصة وفقاً لمبدأ التعاون الدولي.

أما الجزء الثاني من هذا العهد فيتعلق بتعهد الدول الموقعة عليه احترام حقوق الإنسان لجميع الأفراد الموجودين على أراضيها دون أي تمييز بسبب العرق أو اللون أو الجنس أو اللغة أو الدين أو الرأي سياسياً كان أم غير سياسي، أو الأصل القومي أو الاجتماعي، أو الثروة أو النسب أو غير ذلك من الأسباب. ونص الجزء نفسه على ضرورة أن تقوم الدول بتعديل تشريعاتها وقوانينها إذا كانت لا تكفل فعلاً إعمال الحقوق المعترف بها في هذا العهد، بأن تتخذ طبقاً لإجراءاتها الدستورية ولأحكام هذا العهد ما يكون ضروريا لهذا الإعمال من تدابير تشريعية أو غير تشريعية. بالإضافة إلى احترام المحاكمة العادلة لكل من يتعرض للظلم. وكذلك حق المساواة بين الرجال والنساء في التمتع بجميع الحقوق المدنية والسياسية. كما نظّم العهد في هذا الجزء كيفية التعامل مع الحقوق المدنية والسياسية في حالة تعرض الدول لأزمات استثنائية.

ونظم الجزء الثالث من هذا العهد حق الحياة الذي على القوانين حماية هذا الحق والتعامل معه في مختلف هذه الظروف. كما نظّم أيضاً حق الفرد في عدم التعرّض للتعذيب أو المعاملة والعقوبة القاسية واللاإنسانية أو الحاطة بالكرامة من خلال تحديد إجراءات الإيقاف. وكذلك تحريم العبودية والاتجار بالرقيق وحق الإنسان في الحرية والأمان، والتنقل وحرية اختيار مكان إقامته. [1]

أيضاً نظم الجزء الثالث حق حرية الفكرة والوجدان والدين. وحظر أية دعوة للكراهية القومية أو العنصرية أو الدينية تشكل تحريضاً على التمييز أو العداوة أو العنف. وأقر كذلك الحق في التجمع السلمي وضرورة أن يتم تنظيمه من خلال القانون لصيانة الأمن القومي والسلامة العامة والنظام العام وحماية الصحة العامة والآداب العامة وحماية حقوق الآخرين وحرياتهم. ومن الحقوق التي نظمها هذا

[1]- معهد البحرين للتنمية السياسية، الموقع الرسمي،2025/06/18 الرابط:
https://www.bipd.org/publications/Articles/87753.aspx

الجزء أيضاً حق الفرد في تشكيل الجمعيات ومؤسسات المجتمع المدني المختلفة. وحق تكوين الأسرة وحماية حقوق الزوجين المتعددة. وحق الجنسية، وحق المساواة أمام القانون للأفراد، وحقوق الأقليات.

كما تناول العهد الدولي الخاص بالحقوق المدنية والسياسية في الجزء الرابع منه تشكيل اللجنة المعنية بحقوق الإنسان المعنية بمتابعة احترام الدول للحقوق الواردة في العهد نفسه، وإجراءات المتابعة الدورية. أما بالنسبة للجزأين الخامس والسادس فإنه ما يتعلقان بكيفية التوقيع على العهد الدولي، ومسؤولية الأمم المتحدة على الإشراف على هذه الوثيقة الدولية، وكيفية تفسير بنوده والإجراءات المرتبطة بها.

من هنا نلاحظ أن العهد الدولي الخاص بالحقوق المدنية والسياسية يتناول عدداً كبيراً من حقوق الإنسان التي نظمها والتي أخذت بها دساتير الدول الموقعة عليه. [1]

من خلال استقرائنا للمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية تُعد حماية الخصوصية أحد أبرز الحقوق الأساسية التي نصّ عليها القانون الدولي، وتكفلها بشكل صريح إحدى المواد الجوهرية في العهد الدولي الخاص بالحقوق المدنية والسياسية. هذه المادة تُلزم الدول بحماية الأفراد من أي تدخل تعسفي أو غير قانوني في حياتهم الخاصة(1)، بما يشمل شؤون الأسرة، والسكن، والمراسلات، والشرف، والسمعة.

ومع التحول نحو العصر الرقمي، أصبح لهذا النص القانوني بُعد جديد ومعقّد، إذ لم تعد انتهاكات الخصوصية تقتصر على الأساليب التقليدية كالمراقبة المادية أو التنصت المباشر، بل امتدت إلى ممارسات رقمية أكثر تطورًا وخطورة. يشمل ذلك تتبع الأفراد إلكترونيًا عبر المواقع التي يزورونها، وتحليل بياناتهم الشخصية من خلال التطبيقات الذكية، واستخدام تقنيات الذكاء الاصطناعي للتعرف على السلوك والميول والآراء، بل حتى مراقبة تحركاتهم عبر الأجهزة المحمولة والكاميرات الذكية المدمجة.

في هذا السياق، يُعد احترام هذه المادة أمرًا ضروريًا لضمان حماية الحياة الخاصة في ظل ثورة المعلومات. فالتكنولوجيا الحديثة، رغم ما تقدّمه من تسهيلات، أصبحت وسيلة للسيطرة الخفية على حياة الأفراد، تُستخدم أحيانًا من قبل السلطات العامة، وأحيانًا أخرى من قبل الشركات التجارية العملاقة التي تستثمر البيانات الشخصية في الإعلانات، أو تسوّقها لجهات ثالثة دون علم المستخدم.

من هنا، لا تقتصر مسؤولية الدولة على الامتناع عن انتهاك الخصوصية، بل تشمل أيضًا واجبها في تنظيم المجال الرقمي وفرض رقابة صارمة على الفاعلين فيه. فالدولة مُلزمة بوضع تشريعات تُلزم

[1]- انظر المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية

الشركات بالتعامل بشفافية مع بيانات المستخدمين، وتمنع جمع أو استعمال المعلومات الشخصية دون موافقة واضحة ومستنيرة. كما عليها أن تضمن وجود آليات فعالة للرقابة والمساءلة، تُتيح للمواطنين التظلّم في حال تعرضهم لانتهاك خصوصيتهم.

وتزداد أهمية هذه المادة في ضوء المخاطر المتزايدة المرتبطة بتقنيات التعرف على الوجه، والتتبع الجغرافي، وتحليل البيانات الضخمة، وهي أدوات يمكن أن تُستخدم – إن لم تُضبط قانونيًا – في بناء مجتمعات المراقبة الشاملة، حيث يصبح كل تحرك أو رأي خاضعًا للرصد والمحاسبة.

لذلك، فإن احترام هذه المادة وتفعيل مضمونها في السياق الرقمي لا يُعد فقط مطلبًا قانونيًا، بل ضرورة لحماية كرامة الإنسان، وضمان حرية الرأي، والحد من الاستبداد التكنولوجي. إنها تمثل الحاجز القانوني الذي يقف بين حرية الفرد وسلطة المراقبة، سواء كانت حكومية أو تجارية، وتفرض على الجميع – دولةً وسوقًا – حدودًا أخلاقية وقانونية في التعامل مع الحياة الرقمية للأفراد.

باختصار، إن هذه المادة تُعيد التذكير بأن التقدم التكنولوجي لا يُبرر انتهاك الخصوصية، وأن الحقوق الأساسية يجب أن تبقى ثابتة مهما تطورت الوسائل.[1]

أما تحليلنا للمادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية التي تعد من أبرز الدعائم القانونية لحرية الرأي والتعبير، حيث أرست الأساس الدولي لهذا الحق، مؤكدة على عدم جواز تقييده تعسفًا أو تحت أي ذريعة غير مشروعة. فحرية الرأي وفق هذا النص تُعد حقًا مطلقًا لا يجوز المساس به، حتى في حالات الطوارئ، أما حرية التعبير فهي حق محمي، لكنه يقبل بعض القيود المشروعة إذا ما استوفت شروط الضرورة والتناسب وفقًا للقانون.

في السياق الرقمي، تكتسب هذه المادة أهمية متجددة، إذ أصبحت الوسائط الإلكترونية مثل الإنترنت، ومنصات التواصل الاجتماعي، والمدونات الشخصية، الوسيلة الأساسية للتعبير عن الآراء وتداول المعلومات. وقد أكدت لجنة حقوق الإنسان بالأمم المتحدة في تعليقها العام رقم 34 لسنة 2011، أن مضمون المادة 19 يشمل جميع أشكال التعبير الرقمية، بما في ذلك تلك التي تتم عبر الوسائط التكنولوجية الحديثة، مما يمنح بعدًا قانونيًا واضحًا لما يعرف بـ "حرية التعبير الرقمية".

ومع تنامي الحضور الرقمي في الحياة اليومية، أصبحت هذه المادة مرجعًا أساسيًا للمدافعين عن حرية الإنترنت، والناشطين الحقوقيين، في مواجهة موجات الرقابة على المحتوى، أو الحجب، أو محاولات تقنين الرأي العام عبر الفضاء الافتراضي. غير أن الفقرة المتعلقة بالقيود القانونية تمنح الدول

[1]- انظر: أحمد عبد الحفيظ الحسيني، *الحق في حرية الرأي والتعبير في القانون الدولي لحقوق الإنسان*، دار النهضة العربية، القاهرة، 2016، ص. 143.

هامشًا لوضع تشريعات تنظم هذا الحق، بشرط أن تلتزم بضوابط صارمة: أن تكون القيود منصوصًا عليها بالقانون، وأن تكون ضرورية لحماية مصلحة مشروعة كالأمن العام أو الآداب العامة، وأن تتسم بالتناسب.[1]

ومن هذا المنطلق، فإن الموازنة بين تنظيم البيئة الرقمية وبين احترام حرية التعبير تُعد من التحديات الأساسية أمام المشرّع المعاصر. فالدول لا تملك فقط واجب احترام هذا الحق، بل تلتزم أيضًا بتوفير الضمانات الفعلية لحمايته، سواء من انتهاكات الدولة أو من ممارسات المنصات الرقمية الكبرى التي قد تتورط في تقنين الحذف أو تقييد المحتوى دون معايير واضحة.

وبذلك، تمثل المادة 19 مرجعية قانونية دولية تُلزم الدول بأن تراعي عند وضع سياساتها الرقمية التزاماتها في مجال حقوق الإنسان، بما في ذلك ضمان الوصول إلى المعلومات، وحرية التعبير، ورفض الرقابة الإلكترونية المفرطة أو التتبع غير القانوني.

وتشكل **المادتان 21 و22 من العهد الدولي الخاص بالحقوق المدنية والسياسية** إطارًا قانونيًا دوليًا جوهريًا لحماية **الحق في التجمع السلمي وحرية تكوين الجمعيات**، باعتبارهما من الركائز الأساسية في بناء مجتمع مدني فعّال، وضمان المشاركة المجتمعية في الحياة العامة. وقد أكدت هاتان المادتان على أن ممارسة هذين الحقين يجب أن تتم بحرية، ولا يمكن تقييدهما إلا وفق شروط مشددة، تُراعي ضرورة أن تكون أي قيود مفروضة واردة في القانون، ومتماشية مع ما يفرضه مجتمع ديمقراطي من موازنة دقيقة بين الحريات وحماية النظام العام، أو الأمن القومي، أو الصحة العامة، أو حقوق الغير.

في العصر الرقمي، تتجلى أهمية هذين الحقين بشكل خاص، إذ أصبحت المنصات الإلكترونية وسيلة مركزية لتنظيم التجمعات والاحتجاجات، ولتأسيس الجمعيات والمبادرات المجتمعية، خصوصًا في الدول التي تُقيّد النشاط في الفضاء العام التقليدي. إلا أن هذا التوسع في ممارسة الحقوق من خلال الوسائط الرقمية يقابله ازدياد في حجم الانتهاكات، التي تتخذ أشكالًا متعددة، من أبرزها **قطع الإنترنت أو حجب منصات التواصل الاجتماعي أثناء المظاهرات**، بهدف منع التنسيق بين النشطاء، أو إخفاء الانتهاكات عن الرأي العام الدولي. وتُعد هذه الممارسات انتهاكًا واضحًا للمعايير التي أرستها المادتان، حيث أنها تعرقل بشكل تعسفي قدرة الأفراد على التجمع السلمي والتعبير الجماعي.

كما أن استخدام القوانين الفضفاضة لتجريم إنشاء المجموعات الإلكترونية أو المنتديات الرقمية، بحجج مثل "التحريض على الفوضى"، أو "تهديد الأمن العام"، يعكس توظيفًا غير مشروع للسلطة

[1]- نفس المرجع، ص 150

التشريعية بهدف تقييد الفضاء المدني، خاصة عند غياب الأدلة أو المحاكمات العادلة. وتشير حالات كثيرة إلى أن مجرد إنشاء صفحة على منصة مثل "فيسبوك" بهدف مناقشة قضايا اجتماعية أو سياسية يمكن أن يؤدي بصاحبها إلى الاعتقال أو الملاحقة القانونية، وهو ما يتعارض بشكل مباشر مع **الحق في تكوينالجمعيات**، كما كفلته المادة 22، سواء تم هذا التنظيم في الواقع أو عبر الإنترنت.

ورغم أن القانون الدولي يعترف بإمكانية فرض قيود على هذه الحقوق، إلا أن **اللجنة المعنية بحقوقالإنسان بالأمم المتحدة** شددت في تعليقاتها العامة على ضرورة أن تكون هذه القيود **قانونية، ضرورية، ومتناسبة**، وألا تُستخدم كأداة لقمع المعارضة أو تقييد الحريات الأساسية. وهذا ما يجعل حظر التطبيقات والمنصات، أو الملاحقة بسبب النشاط الرقمي الجماعي، مخالفًا لروح الالتزامات الدولية للدول الأطراف في العهد.

إن ما نشهده اليوم من تحوّل التكنولوجيا إلى أداة رقابة، بدلًا من أن تكون فضاءً للحرية، يعكس الحاجة الملحّة إلى تطوير إطار حقوقي فعال يضمن حماية هذه الحريات في المجال الرقمي، ويضع حدًا للاستخدام المفرط لذرائع الأمن القومي أو النظام العام لتبرير القيود التعسفية.[1]

المطلب الثاني: الصكوك الدولية الخاصة بالحقوق الرقمية

تُعد اتفاقية بودابست لعام 2001 أول إطار دولي لمكافحة الجرائم الإلكترونية وتعزيز التعاون بين الدول في هذا المجال. أما اللائحة العامة لحماية البيانات (GDPR) التي أقرها الاتحاد الأوروبي سنة 2016، فتهدف إلى حماية البيانات الشخصية وضمان خصوصية الأفراد. ويُشكل كل منهما دعامة قانونية مهمة في مواجهة التحديات الرقمية المعاصرة.

الفرع الاول: اتفاقية بودابست

تعد اتفاقية بودابست اتفاقية دولية تُعنى بمكافحة الجرائم الإلكترونية، وقد وُضعت في إطار مجلس أوروبا. تهدف الاتفاقية إلى توحيد التشريعات الوطنية وتعزيز التعاون القضائي العابر للحدود. وتُشكل مرجعًا دوليًا رئيسيًا لمعالجة التحديات القانونية في الفضاء الرقمي.

أولا- مضمون الاتفاقية

تتكون اتفاقية بودابست لمكافحة الجرائم الإلكترونية، التي اعتمدها مجلس أوروبا سنة 2001، من 48 مادة موزعة على عدة أبواب رئيسية. وتهدف الاتفاقية إلى وضع إطار قانوني موحد يعالج مختلف أنواع الجرائم المرتبطة باستخدام تكنولوجيا المعلومات، مع مراعاة احترام الحقوق الأساسية

[1]- انظر نص اتفاقية بوداباست ، تاريخ التصفح، 2025/06/18، متاح على الموقع :
https://www.coe.int/en/web/cybercrime/the-budapest-convention

للأفراد. وقد أصبحت هذه الاتفاقية مرجعًا عالميًا تستخدمه العديد من الدول لتطوير قوانينها الوطنية في المجال الرقمي.

في الباب الأول، المكوَّن من المادتين 1 و2، يتم التركيز على التعريفات والمفاهيم التقنية الأساسية لضمان انسجام الفهم القانوني بين الدول الأطراف. فمثلًا، تنص المادة 1 على تعريف "نظام الحاسوب"(1) بأنه أي جهاز أو مجموعة أجهزة مترابطة تُستخدم لمعالجة البيانات آليًا. أما المادة 2، فتُلزم الدول الأعضاء بتجريم الوصول غير المشروع إلى الأنظمة المعلوماتية، وهو ما يُعتبر الأساس القانوني لمحاربة القرصنة أو ما يُعرف بـ"Hacking"، حيث يشترط أن يتم الدخول إلى النظام بشكل متعمد ودون إذن.[1]

أما الباب الثاني، الذي يمتد من المادة 3 إلى المادة 11، فيمثل الجانب الردعي من الاتفاقية. وهو يُحدّد الجرائم التي يجب أن تُعتبر أفعالًا إجرامية بموجب القانون الجنائي الوطني للدول المصادقة. تبدأ المادة 3 بتجريم اعتراض البيانات الرقمية، مثل التنصت على الاتصالات الإلكترونية دون ترخيص قانوني، مما يُعزز حماية الخصوصية على الإنترنت. وتليها المادة 4 التي تُجرّم التعديل أو الحذف أو الإتلاف المتعمد للبيانات الحاسوبية، وهو ما يُعد انتهاكًا لسلامة البيانات.[2]

وتُضاف إلى ذلك المادة 5، التي تجرّم أي فعل يؤدي إلى تعطيل عمل نظام معلوماتي، مثل الهجمات الإلكترونية التي تهدف إلى شل المؤسسات أو المواقع الحكومية. أما المادة 6، فتُجرّم تصنيع أو توزيع الأدوات أو البرمجيات المصممة خصيصًا لارتكاب جرائم إلكترونية، كأدوات اختراق الأنظمة أو سرقة المعلومات.

يمتد نطاق الاتفاقية ليشمل الجرائم المرتبطة بالمحتوى الرقمي في المواد من 7 إلى 11. فالمادة 7 تتناول جرائم التزوير الإلكتروني، أي إنشاء أو تعديل بيانات بهدف استخدامها بشكل احتيالي كما لو كانت أصلية. وتليها المادة 8 التي تُعنى بالاحتيال الإلكتروني، مثل استخدام البرامج أو الأنظمة لتحقيق مكاسب غير مشروعة. وتُخصص المادة 9 لتجريم إنتاج أو توزيع أو حيازة مواد إباحية متعلقة بالأطفال، وهو ما يُعد من أشد الانتهاكات في الفضاء الرقمي. كما تنص المادة 10 على حماية حقوق الملكية الفكرية، وتجريم نسخ أو توزيع محتوى رقمي محمي بدون إذن. وأخيرًا، تُلزم المادة 11 الدول بتجريم كل من يشارك أو يحرض أو يحاول تنفيذ أي من الجرائم السابقة.[3]

[1]- انظر: نفس المرجع
[2]- انظر: نفس المرجع
[3]- انظر: نفس المرجع

من خلال هذه المنظومة المتكاملة، تُبرز اتفاقية بودابست شموليتها في التعامل مع الجرائم الإلكترونية، إذ لم تقتصر على حماية الأنظمة التكنولوجية، بل شملت أيضًا حماية الحقوق الرقمية للأفراد، مثل الحق في الخصوصية، وسلامة البيانات، والملكية الفكرية. كما أنها تضع الأسس القانونية للتعاون الدولي في مكافحة الجرائم العابرة للحدود.

ثانيا- أبرز أهداف اتفاقية بودابست

تسعى اتفاقية بودابست لمكافحة الجرائم الإلكترونية إلى تحقيق مجموعة من الأهداف الجوهرية التي تجعل منها أداة فاعلة في التصدي للتحديات القانونية التي تفرضها البيئة الرقمية الحديثة. ومن أبرز هذه الأهداف، تحقيق التجانس التشريعي بين الدول في مجال الجرائم السيبرانية، وهو ما يُعد شرطًا أساسيًا لضمان فعالية التعاون الدولي.

ولتجسيد هذا الهدف، وضعت الاتفاقية **معايير دنيا** موحدة ينبغي على الدول الأطراف إدراجها في قوانينها الوطنية. ويُلاحظ أن الباب الثاني من الاتفاقية، وخاصة المواد من المادة 2 إلى المادة 11، يقدم مجموعة من الأفعال التي تُعد جرائم بموجب الاتفاقية، مثل الوصول غير المشروع إلى الأنظمة (المادة 2)، اعتراض البيانات (المادة 3)، التدخل في البيانات أو الأنظمة (المادتان 4 و5)، وإساءة استخدام الأدوات (المادة 6)، فضلًا عن الجرائم المتعلقة بالتزوير، الاحتيال، المواد الإباحية الخاصة بالأطفال، وانتهاك حقوق الملكية الفكرية (المواد 7 إلى 10). هذا التحديد الدقيق يهدف إلى منع تباين القوانين من حيث التجريم والعقوبة.

ويُسهم هذا التنسيق التشريعي في تسهيل مجموعة من الإجراءات القانونية الدولية، أبرزها:

- تسليم المجرمين بين الدول الأطراف، وهو ما تؤطره الاتفاقية بشكل غير مباشر من خلال المطالبة بتجريم الأفعال ذاتها في القوانين المحلية.
- تعزيز المساعدة القضائية المتبادلة، وهو ما تنص عليه صراحةً المادة 25 التي تلزم الدول بتبادل المعلومات وتقديم العون القانوني في التحقيقات والملاحقات القضائية المرتبطة بالجرائم الإلكترونية.
- تقليص الفجوات القانونية التي قد تُستغل من قبل المجرمين للفرار من الملاحقة، خاصة أن الجرائم الرقمية تتصف بكونها عابرة للحدود، ولا تتقيد بالنطاق الإقليمي للدولة.

من هذا المنظور، تُعد الاتفاقية أداةً لا غنى عنها لبناء ثقة قانونية متبادلة بين الدول، وهي تسهم في التغلب على العقبات القانونية والإجرائية التي كانت تعوق التعاون الدولي في مجال مكافحة الجرائم

الإلكترونية. كما تعزز الالتزام الجماعي بإنشاء بيئة رقمية آمنة، من خلال ربط الجهد الوطني بالمستوى الدولي في التشريع والتطبيق والمساءلة.[1]

ثالثا- اتفاقية بودابست من النطاق الإقليمي الي النطاق العالمي

على الرغم من أن اتفاقية بودابست قد وُضعت في إطار مجلس أوروبا، فإن نطاقها لم يقتصر على الدول الأوروبية، بل فُتحت أيضًا أمام دول من خارج القارة، في اعتراف صريح بالطابع العالمي للجرائم الإلكترونية. وقد ساهم هذا الانفتاح في تعزيز مكانة الاتفاقية كمرجع دولي شامل للتشريعات السيبرانية.

ويُعد انضمام **المغرب** إلى الاتفاقية في 29 يونيو 2018، خطوة بارزة، حيث أصبحت أول دولة عربية تنضم رسميًا إليها، وقد دخلت الاتفاقية حيّز التنفيذ في المغرب بداية من 1 أكتوبر 2018. ويعكس هذا الانضمام رغبة المملكة في التفاعل مع المنظومة الأوروبية والدولية من أجل تطوير قدراتها القانونية والمؤسساتية لمكافحة الجرائم السيبرانية.

أما**الولايات المتحدة الأمريكية**، ورغم كونها ليست عضوًا في مجلس أوروبا، فقد وقعت الاتفاقية في 23 نوفمبر 2001، وصادقت عليها في 29 سبتمبر 2006، لتدخل حيز التنفيذ لديها في 1 يناير 2007. ويُبرز هذا الموقف الأمريكي أهمية الاتفاقية في تشكيل إطار قانوني عالمي لمكافحة الجرائم الإلكترونية، يتجاوز الحدود الإقليمية ويتماشى مع التحديات المشتركة التي تواجهها مختلف الدول في الفضاء الرقمي.[2]

رابعا- نتائج الاتفاقية

أحدثت اتفاقية بودابست تحولًا نوعيًا في كيفية تعامل القانون الدولي مع التحديات الجديدة التي تطرحها تكنولوجيا المعلومات والاتصالات. فقد أكدت الاتفاقية، من خلال أحكامها، على ضرورة الاعتراف بوجود فضاء قانوني رقمي مستقل، يتطلب تطوير قواعد خاصة وآليات مبتكرة لمواجهته.

وتتجلى أبرز نتائج الاتفاقية في إرساء **نموذج قانوني مرن وعابر للحدود**، من خلال دعم آليات التعاون الدولي، سواء في تبادل المعلومات والأدلة الرقمية، أو في **تسليم المجرمين**، أو في إجراء **التحقيقات المشتركة** بين الدول الأطراف. وتُعد هذه الممارسات حيوية في التصدي لجرائم لا تعترف

[1]- انظر: **الحمادي طارق**، *الجرائم الإلكترونية في القانون الدولي والوطني: دراسة مقارنة*، دار الجامعة الجديدة للنشر، القاهرة، 2009، ص 115.
[2]- انظر: المرجع نفسه ص 117.

بالحدود الجغرافية، مثل الاختراقات السيبرانية، والاحتيال الرقمي، والاستغلال الجنسي للأطفال عبر الإنترنت.

كما أن الاتفاقية تمهد الطريق لإبرام **بروتوكولات إضافية** تستجيب لتطور طبيعة التهديدات الرقمية، سواء تلك المتعلقة بـ**الإرهاب السيبراني**، أو **الذكاء الاصطناعي المستخدم لأغراض إجرامية**، أو **جرائم الاستغلال الإلكتروني للأطفال**.وبذلك، فإن اتفاقية بودابست لا تمثل فقط آلية قانونية قائمة، بل هي إطار قابل للتطور والتوسعة، يُواكب باستمرار التحولات السريعة التي يشهدها العالم الرقمي.[1]

الفرع الثاني: اللائحة العامة لحماية البيانات GDPR

اللائحة العامة لحماية البيانات (GDPR) هي قانون أوروبي يحمي خصوصية الأفراد. تنظم كيفية جمع واستخدام البيانات الشخصية. وتهدف إلى منح الناس مزيدًا من السيطرة على معلوماتهم.

أولا- الإطار العام للائحة GDPR

اللائحة العامة لحماية البيانات (GDPR) تُعد الإطار التشريعي الأساسي في الاتحاد الأوروبي لحماية البيانات الشخصية، وقد دخلت حيز التنفيذ في 25 مايو 2018. تهدف هذه اللائحة إلى حماية الحقوق والحريات الأساسية للأفراد، لا سيما حقهم في حماية بياناتهم الشخصية، كما ورد في **المادة 1** التي تُؤكد على أن الهدف الأساسي من اللائحة هو حماية الأفراد في ما يخص معالجة بياناتهم وضمان حرية انتقال هذه البيانات.

أما **المادة 2**، فقد حددت نطاق تطبيق اللائحة من حيث الموضوع، حيث تُطبق على المعالجة الآلية أو اليدوية للبيانات الشخصية التي تُعد جزءًا من نظام ملفات، سواء كانت إلكترونية أو ورقية، مع بعض الاستثناءات مثل المعالجة لأغراض أمنية أو دفاعية أو دينية بحتة.

بينما تُوسّع **المادة 3** من نطاق التطبيق الإقليمي، إذ تُلزم أي مؤسسة خارج الاتحاد الأوروبي بالامتثال لمقتضيات اللائحة إذا كانت تقدم خدمات أو تراقب سلوك الأفراد داخل الاتحاد، وهو ما يجعل اللائحة ذات طابع عابر للحدود.

تُشكل هذه المواد الثلاث الأساس القانوني العام الذي تقوم عليهGDPR ، حيث ترسم حدود تطبيقها القانوني والمكاني، وتُؤكد على أولوية حماية الفرد في البيئة الرقمية المتطورة.[2]

[1]- انظر الموقع الرسمي،اللائحة العامة لحماية البيانات، الرابط:https://gdpr-info.eu
[2]- انظر: نفس المرجع

ثانيا- مبادئها الأساسية

يشكّل الباب الثاني من اللائحة العامة لحماية البيانات (GDPR) الركيزة الأساسية للفلسفة التشريعية الأوروبية في تنظيم كيفية التعامل مع البيانات الشخصية، إذ يضع المبادئ والقواعد التي يجب أن تحكم كل عملية معالجة للبيانات.

تعد **المادة 5** من هذا الباب حجر الأساس في تحديد المبادئ الجوهرية لمعالجة البيانات، حيث تُلزم

الجهات المعنية بالتقيد بجملة من الضوابط، أبرزها:

- **الشرعية، والشفافية، والعدل:** يجب أن تُعالج البيانات في إطار قانوني واضح، وأن يكون أسلوب المعالجة مفهوماً وشفافاً بالنسبة لصاحب البيانات.

- **تحديد الغاية:** ينبغي ألا تُستخدم البيانات إلا للأغراض التي جُمعت من أجلها بشكل صريح ومسبق، ما يمنع أي توسّع غير مشروع في الأهداف.

- **تقليل البيانات:** لا يجوز جمع بيانات تفوق الحد اللازم لتحقيق الغاية المرجوة.

- **الدقة** :يجب ضمان تحديث البيانات وتصحيح أي معلومات خاطئة أو غير دقيقة.

- **تحديد مدة الاحتفاظ:** تُحظر الاحتفاظ بالبيانات لمدة أطول مما تفتضيه الحاجة العملية أو القانونية.

- **السلامة والسرية:** تُلزم المعالجة باتخاذ إجراءات أمنية وتقنية كافية لحماية البيانات من الوصول غير المصرح به، أو التلاعب، أو التسريب.

أما **المادة 6**، فتبين الأسس القانونية التي تُبرر المعالجة، والتي تشمل: الحصول على **الموافقة**، أو ضرورة تنفيذ **عقد**، أو **الامتثال لالتزام قانوني**، أو حماية **مصالح حيوية**، أو تحقيق **مصلحة عامة**، أو الاستناد إلى **مصلحة مشروعة** بشرط ألا تتعارض مع حقوق وحريات الفرد.

وفي السياق ذاته، تُفصّل **المادة7** شروط صحة "الموافقة" بوصفها أحد أبرز الأسس القانونية للمعالجة، حيث يجب أن تكون الموافقة **حرة الإرادة، ومحددة، ومبنية على وعي مسبق، وقابلة للإثبات**.

أما **المادة 9**، فقد شددت على حماية **البيانات الحساسة** مثل المعتقدات الدينية، والحالة الصحية، والميول الجنسية، حيث منعت معالجتها كأصل عام، إلا في حالات استثنائية محدودة وبضوابط صارمة، وذلك لما تنطوي عليه من خطر كبير على الحقوق الشخصية في حال إساءة استخدامها.[1]

كما نصّت **المادة 10** على حظر معالجة البيانات المتعلقة **بالإدانات الجنائية أو المخالفات** دون توافر ضمانات قانونية كافية، ما يعكس حرص المشرّع الأوروبي على تجنب أي إساءة في استخدام تلك البيانات التي قد تمس السمعة أو الحرية الشخصية للفرد.

ثالثا- حقوق الافراد أصحاب البيانات

يُولي الباب الثالث من اللائحة العامة لحماية البيانات (GDPR) أهمية كبيرة لحقوق الأفراد، حيث لا يُنظر إليهم كمجرد "موضوعات بيانات" بل كأطراف فاعلة تملك سيطرة حقيقية على معلوماتها الشخصية. تنص هذه المواد على مجموعة من الحقوق الأساسية التي تهدف إلى تعزيز الشفافية، والمساءلة، وتمكين الأفراد من التحكم في بياناتهم.

تبدأ المادة 12 بالتأكيد على ضرورة وضوح المعلومات المقدمة للأفراد، وتُلزم المؤسسات بشرح كيفية استخدام البيانات بلغة بسيطة وسهلة الفهم. أما المادتان 13 و14 فتُحددان التزامات المؤسسات في إعلام الأشخاص عند جمع بياناتهم، سواء بشكل مباشر أو غير مباشر، مع توضيح الغرض من الاستخدام، والجهات التي ستتلقى البيانات، ومدة الاحتفاظ بها، إضافة إلى توضيح حقوق الفرد.

واستنادًا إلى المادة 15، يتمتع الأفراد بحق الوصول إلى بياناتهم، بما في ذلك الحصول على نسخة منها ومعرفة كيفية معالجتها. ويكفل الحق في التصحيح (المادة 16) للأفراد إمكانية تعديل أية معلومات غير دقيقة أو ناقصة، في حين تتيح المادة 17، المعروفة بـ"الحق في النسيان"، إمكانية حذف البيانات إذا لم تعد هناك حاجة قانونية أو عملية للاحتفاظ بها، أو إذا سحب الفرد موافقته.

من جهة أخرى، تُخوّل المادة 18 الأفراد بتقييد معالجة بياناتهم مؤقتًا في ظروف معينة، بينما تمنح المادة 20 ما يُعرف بـ"حق نقل البيانات"، وهو تمكين الفرد من نقل بياناته من مزوّد خدمة إلى آخر بصيغة قابلة للقراءة آليًا. وتُكرّس المادة 21 الحق في الاعتراض على معالجة البيانات، لا سيما في حالات التسويق المباشر، وهو ما يُعزز حماية المستخدمين من الاستخدامات التجارية غير المرغوبة.

[1]- انظر: نفس المرجع

أخيرًا، تُقيّد المادة 22 القرارات التي تُتخذ بصورة آلية بالكامل (كالتي تُتخذ عبر الخوارزميات)، خصوصًا عندما يكون لهذه القرارات أثر قانوني أو جوهري على الشخص، مما يُمثل خطوة مهمة في مواجهة مخاطر الذكاء الاصطناعي والتحليل الآلي.

بهذا، يُشكل هذا الباب حجر الزاوية في حماية الخصوصية الرقمية، ويعكس تحولًا عميقًا في فهم العلاقة بين الأفراد ومؤسسات جمع البيانات[1]

رابعا-التزامات المؤسسات المعالجة للبيانات

يُسلط الباب الرابع من اللائحة العامة لحماية البيانات (GDPR) الضوء على المسؤوليات القانونية والتنظيمية للمؤسسات التي تقوم بجمع أو معالجة البيانات الشخصية، ويُعد هذا القسم جوهريًا في تحقيق مبدأ المساءلة .فبدلًا من الاقتصار على فرض قيود، تُطالب اللائحة المؤسسات بإثبات التزامها النشط بقواعد حماية البيانات.

تنص المادة 24 على أن المؤسسات مسؤولة عن إثبات امتثالها للمبادئ الأساسية المنصوص عليها في المادة 5، مثل مشروعية المعالجة، وتحديد الغرض، وتقليل البيانات، والدقة. أما المادة 25، فتُدخل مبدأ "الخصوصية حسب التصميم والافتراض"، والذي يوجب على المؤسسات إدماج حماية الخصوصية في البنية التحتية التقنية والعملية منذ بداية تطوير الخدمات، وليس بعد حدوث المخاطر.

وتُطالب المادة 30 بضرورة إنشاء سجل مفصل لكافة أنشطة معالجة البيانات داخل المؤسسة، وهو ما يُعدّ أداة تنظيمية مهمة لتتبع كيفية التعامل مع المعلومات. وتؤكد المادة 32 على وجوب اتخاذ تدابير تقنية وتنظيمية مناسبة لحماية البيانات، مثل التشفير، وضبط صلاحيات النفاذ، وغيرها من أدوات الأمان.

في حال حدوث اختراق أو خرق للبيانات، تُلزم المادة 33 المؤسسات بإبلاغ الجهة الرقابية خلال 72 ساعة كحد أقصى، أما المادة 34 فتُلزم بإبلاغ الأشخاص المتضررين إذا كان الانتهاك من شأنه أن يُهدد حقوقهم أو حرياتهم بشكل كبير، مثل سرقة الهوية أو فقدان البيانات الحساسة.

كما تُلزم المادة 35 بإجراء "تقييم أثر حماية البيانات (DPIA) "قبل البدء في أي نشاط معالجة يُحتمل أن يُشكل خطرًا عاليًا على خصوصية الأفراد، وهو ما يُمثل خطوة وقائية مهمة. ووفقًا لـ

[1]- انظر: نفس المرجع

المادة37، يُطلب من المؤسسات الكبرى أو التي تتعامل مع بيانات حساسة أن تُعيّن "مسؤولًا لحماية البيانات (DPO) "يشرف على التزام المؤسسة باللائحة.

وأخيرًا، تدعو المواد 40 إلى43 إلى تطوير واعتماد "مدونات سلوك" و"شهادات اعتماد" لحماية البيانات، بما يُساعد على تحسين الالتزام الطوعي من قبل المؤسسات، ويُوفر إطارًا موثوقًا للثقة بين الشركات والجمهور.

بهذا، يبرز هذا الباب كيف أن GDPR لا يكتفي بتحديد الحقوق، بل يضع أيضًا مسؤوليات واضحة على الجهات المعالجة، لضمان الشفافية، والأمان، والمساءلة في كل مرحلة من مراحل التعامل مع البيانات الشخصية[1]

الفرع الخامس: الإطار التنظيمي والرقابي

تُشكّل الأبواب من الخامس إلى الثامن من اللائحة العامة لحماية البيانات (GDPR) الإطار العملي والتنفيذي الذي يضمن تطبيق المعايير والمبادئ المتعلقة بحماية البيانات الشخصية، ويُعالج قضايا حيوية مثل نقل البيانات خارج الاتحاد الأوروبي، وتحديد صلاحيات الرقابة، وآليات الإنفاذ، والعقوبات، ما يجعل هذه الأبواب جوهر النظام القانوني الأوروبي في البيئة الرقمية.

تنظم اللائحة في بابها الخامس نقل البيانات إلى خارج الاتحاد الأوروبي، حيث تُشترط مجموعة من الضوابط الصارمة لتأمين مستوى كافٍ من الحماية عند إرسال البيانات إلى دول أو منظمات دولية. يُسمح بالنقل فقط إذا اعتُرف لتلك الدول بأنها توفّر حماية مكافئة (المادة 45). وإذا لم يكن هناك قرار رسمي من المفوضية الأوروبية، يجب على المؤسسات استخدام ضمانات مناسبة مثل البنود التعاقدية القياسية (المادة 46)، أو ما يسمى بـ "القواعد الملزمة للشركات" في سياق المجموعات متعددة الجنسيات (المادة 47). وتُمنح استثناءات محدودة في حالات الضرورة القصوى أو بموافقة صريحة من صاحب البيانات، وفق المادة 49، مما يضمن عدم إخراج البيانات عن حماية اللائحة إلا في أضيق الحدود.

في الباب السادس، تؤسس اللائحة سلطات رقابية وطنية مستقلة في كل دولة عضو، وفق المادة 51، تتولى مراقبة تنفيذ أحكام القانون. تتمتع هذه السلطات بصلاحيات التحقيق والإنذار وفرض الغرامات، كما تنسق مع السلطات الأخرى عند وجود عمليات معالجة عابرة للحدود، وذلك باستخدام آلية "المشرف الرئيسي" المنصوص عليها في المادة 60. ويُشرف على هذا التعاون "مجلس حماية البيانات الأوروبي(EDPB) "، الذي ينظم العلاقات بين السلطات الوطنية ويوفر التوجيهات العامة (المادة 68).

[1]- انظر: نفس المرجع

كما تُمنح الأفراد، بموجب المواد 77–79، الحق في تقديم شكاوى لدى الجهات الرقابية أو اللجوء للقضاء عند انتهاك حقوقهم.[1]

أما الباب السابع، فيتناول نظام العقوبات والمسؤولية المدنية. تنص المادة 82 على حق الأفراد في المطالبة بالتعويض عن أي ضرر مادي أو معنوي ناتج عن انتهاك لأحكام اللائحة. أما المادة 83، فهي توضح آلية فرض الغرامات الإدارية، التي قد تصل إلى 20 مليون يورو أو 4% من إجمالي الإيرادات العالمية السنوية للشركة المخالفة، أيهما أكبر، بحسب طبيعة المخالفة. كما تتيح المادة 84 للدول الأعضاء سنّ عقوبات إضافية بموجب تشريعاتها الوطنية، ما يعزز الردع على المستوى المحلي.

وأخيرًا، يُعالج الباب الثامن الأحكام الختامية التي تتعلق بحالات خاصة مثل التوفيق بين حماية البيانات وحرية التعبير في الصحافة والبحث الأكاديمي (المادة 85)، واستثناءات مشروطة للمعالجة لأغراض علمية أو تاريخية (المادة 89)، وكذلك التنسيق مع تشريعات أوروبية أخرى مثل توجيه الخصوصية الإلكترونية (المادة 95). وتضمن هذه المواد الانسجام بين حماية البيانات وحقوق أو مصالح مجتمعية أخرى، دون الإخلال بجوهر الحق في الخصوصية[2]

بذلك، توفر هذه الأبواب آلية متكاملة تجعل من اللائحة العامة لحماية البيانات نظامًا متوازنًا وفعالًا، قادرًا على مواجهة التحديات الرقمية العالمية، وحماية الأفراد، وتنظيم عمل المؤسسات، على نحو شفاف وقابل للتنفيذ.

[1]- انظر: نفس المرجع
[2]- مجلس حقوق الإنسان التابع للأمم المتحدة، القرار A/HRC/20/8 (2012)، متاح على الموقع: https://digitallibrary.un.org/?ln=ar

المبحث الثاني: الجهود الدولية المبذولة لحماية الحقوق الرقمية في ظل التحديات الراهنة

في ظل التحولات الرقمية المتسارعة، أصبحت الحقوق الرقمية مهددة من عدة جوانب، أبرزها المراقبة، انتهاك الخصوصية، والهجمات السيبرانية. وقد استدعى ذلك تدخلًا دوليًا متزايدًا لحماية هذه الحقوق، من خلال إصدار اتفاقيات وتطوير أطر تنظيمية متخصصة. تسعى هذه الجهود إلى تحقيق توازن بين حرية الاستخدام الرقمي ومتطلبات الأمن. كما تهدف إلى تعزيز التعاون الدولي لضمان بيئة رقمية آمنة تحترم حقوق الإنسان. يتناول هذا المبحث أبرز المبادرات والآليات الدولية لمواجهة التحديات الرقمية الراهنة.

المطلب الأول: الجهود الدولية المبذولة في حماية الحقوق الرقمية

شهدت حماية الحقوق الرقمية اهتمامًا دوليًا متزايدًا، حيث تم الاعتراف بها كامتداد طبيعي لحقوق الإنسان، خاصة في مجالات الخصوصية وحرية التعبير والوصول إلى المعلومات. وقد ساهمت العديد من المبادرات القانونية والتنظيمية في ترسيخ هذا التوجه، من خلال سن قوانين لحماية البيانات، وتعزيز التعاون الدولي ضد الجرائم الرقمية، ووضع معايير تقنية وأخلاقية لضمان أمن الفضاء الرقمي. كما تُبذل جهود تنسيقية عالمية لتشجيع النقاش حول السياسات الرقمية وضمان التوازن بين الابتكار والحقوق الأساسية.

الفرع الأول: اعتراف الأمم المتحدة بالحقوق الرقمية

لعبت الأمم المتحدة دورًا رائدًا في ترسيخ الحقوق الرقمية ضمن منظومة حقوق الإنسان، واعتبارها امتدادًا لحقوق قائمة مثل الخصوصية، وحرية التعبير، والوصول إلى المعلومات. ففي عام 2012، اعتمد مجلس حقوق الإنسان القرار رقم A/HRC/20/8 الذي جاء فيه أن "الحقوق التي يتمتع بها الأفراد خارج الإنترنت يجب أن تُحمى أيضًا على الإنترنت"، مما أكد أن الفضاء الرقمي ليس خارج نطاق القانون الدولي لحقوق الإنسان.

لاحقًا، صدرت تقارير هامة من المقررين الخاصين، من أبرزها تقرير فرانك لارو (2013)، الذي انتقد الرقابة الرقمية الجماعية، واعتبرها غير متناسبة مع معايير القانون الدولي، مطالبًا بوجود ضمانات قانونية قوية تقيّد سلطة الدول في مراقبة البيانات الخاصة. هذه الوثائق أوجدت مرجعيات حقوقية ملزمة أخلاقيًا، تم البناء عليها في العديد من التشريعات الوطنية والإقليمية لاحقًا[1].

[1]- انظر الموقع الرسمي،اللائحة العامة لحماية البيانات، الرابط:https://gdpr-info.eu

الفرع الثاني: جهود المنظمات الدولية التقنية والتنظيمية

أولا: الاتحاد الدولي للاتصالات(ITU)

هو منظمة تابعة للأمم المتحدة، تعمل على **تنظيم قطاع الاتصالات** عالميًا. يقوم الاتحاد بتقديم الدعم للدول، خاصة النامية منها، من أجل تطوير بنيتها الرقمية بشكل آمن. كما يصدر تقارير مثل **"مؤشر الأمن السيبراني العالمي"**الذي يُقيّم جهود الدول في حماية أنظمتها من التهديدات الرقمية.[1]

ثانيا: الهيئة العامة للأسماء والأرقام المخصصة على الإنترنت (ICANN)

هي الجهة المسؤولة عن تنظيم **أسماء النطاقات على الإنترنت** مثل(.com) و (.org) وتلعب دورًا مهمًا في **ضمان حيادية الإنترنت** وعدم احتكاره من قبل أي جهة، مما يدعم حق المستخدمين في الوصول المفتوح للمعلومات.[2]

ثالثا: منظمة المنظمة الدولية للمعايير(ISO)

تُصدر المنظمة الدولية للمعايير (ISO) العديد من المعايير التقنية العالمية، منها معايير **حماية أمن المعلومات** مثل سلسلةISO/IEC 27000 ، والتي تعتمدها الكثير من الحكومات والشركات لحماية البيانات من القرصنة والتسريب[3]

رابعا: منتدى حوكمة الإنترنت(IGF)

يُعتبر المنتدى فضاءً مفتوحًا وغير ملزم قانونيًا، يجمع بين الحكومات، والشركات، والمنظمات التقنية، والمجتمع المدني، والأكاديميين، من أجل مناقشة السياسات المتعلقة بالإنترنت والحقوق الرقمية، مثل:

- حرية التعبير على الإنترنت
- خصوصية البيانات
- الوصول المفتوح للمعلومات
- أمن الفضاء السيبراني
- الذكاء الاصطناعي وتأثيره على حقوق الإنسان

---

[1]-الموقع الرسمي، الهيئة العامة للأسماء والأرقام المخصصة على الإنترنت، الرابط:
https://www.icann.org/resources/pages/what-2012-02-25-en

[2]- الموقع الرسمي، منظمة المنظمة الدولية للمعايير ،الرابط: -https://www.iso.org/isoiec-27001 :
information-security.html

[3]- **الموقع الرسمي**، منتدى حوكمة الإنترنت، **الرابط:**https://www.intgovforum.org/en/about

المنتدى لا يُصدر قوانين أو معاهدات، بل يعمل من خلال جلسات نقاشية سنوية تُعقد في دول مختلفة، تُشارك فيها وفود رسمية وغير رسمية من كل أنحاء العالم. يُنظّم المنتدى حول مواضيع وقضايا رقمية راهنة، ويُختتم بإصدار توصيات وتقرير نهائي يُعرض على الأمين العام للأمم المتحدة.

ومن بين مواضيعه الحديثة:

- الذكاء الاصطناعي وحقوق الإنسان
- الاقتصاد الرقمي والشفافية
- الأمن السيبراني وبناء الثقة
- الفجوة الرقمية بين الشمال والجنوب

رغم أن IGF ليس جهة تشريعية، إلا أنه يلعب دورًا مهمًا في:

- الضغط على الحكومات والشركات لاحترام الخصوصية وحرية التعبير.
- بناء شبكات تعاون دولية تدافع عن الحقوق الرقمية.
- تمكين منظمات المجتمع المدني من إيصال أصواتها على المستوى الدولي[1]

المطلب الثاني: التحديات التي تواجه اعمال الحقوق الرقمية

يشهد العالم الرقمي تحديات متزايدة تهدد ممارسة الحقوق الرقمية بشكل فعّال وآمن. وتُعد المراقبة الحكومية والتجسس الرقمي من أبرز المخاطر التي تُقيد الحريات وتُعرض الخصوصية للانتهاك. كما تشكل الجرائم الإلكترونية تهديدًا مباشرًا للأفراد والمجتمعات، من خلال سرقة البيانات أو الابتزاز أو بث الكراهية. يتناول هذا المطلب أبرز هذه التحديات وآثارها المتعددة على الحقوق الرقمية.

الفرع الأول: المراقبة الحكومية والتجسس الرقمي

يعتبر الانتشار المتزايد لعمليات المراقبة الحكومية والتجسس الرقمي من أبرز التحديات التي تقف عاتقا امام اعمال الحقوق الرقمية على المستوى الدولي فرغم الاعتراف الدولي بالحق في الخصوصية وحريه التعبير والوصول الى المعلومات الى ان هذه الحقوق تتعرض للانتهاكات المقصودة نتيجة توسع الأجهزة الحكومية في مراقبه الافراد في الفضاء الرقمي دون وجود ضمانات قانونيه فعاله توازن بين الامن واحترام الحقوق

[1]- مريم الشريف، الخصوصية الرقمية في ظل القانون الدولي لحقوق الانسان، مذكره ماستر، جامعه سطيف 2022 صفحه 45

أولا: الرقابة الرقمية وتآكل الخصوصية الرقمية

تعتبر الرقابة الرقمية غير المنظمة قانونيا تهديدا خطيرا للخصوصية الرقمية التي تمثل حقا اساسيا معترفا به على المستوى القانون الدولي تعتمد العديد من الحكومات تقنيات متقدمة لمراقبه الاتصالات الإلكترونية ومتابعه الأنشطة الرقمية للأفراد من غير ضمانات قانونيه واضحة بالحصول على موافقه قضائية مسبقة او إطار التشريعي شفاف يعمل على تنظيم هذه الممارسات هذا الواقع يؤدي الى تآكل تدريجي لحق الخصوصية الرقمية مما يثير مخاوف متزايدة بشأن انتهاك الحريات الفردية في الفضاء الرقمي. [1]

اشاره الباحثة كم فرح ميدان في هذا البيان الى ان غياب إطار الرقابي صلب يجعل هذه الممارسات تخرج عن نطاق المعايير الدولية المتفق عليها مما يخلق حاله من عدم التوازن في متطلبات الامن القومي وحماية الحقوق الفردية (1) كما كشفت دراسة اجراها مركز مينا للحقوق الرقمية في ان التقنيات المستخدمة في المنطقة العربية لأغراض المراقبة غالبا غالبا ما تطبق دون اعلام الافراد المستهدفين مسبقا مما يؤدي الى تقليص ثقة المستخدمين في الفضاء الرقمي وتحد من حريه التعبير والتفاعل عبر الانترنت.[2]

اضافه الى ذلك أبرز تقرير الفضاء الرقمي والحريات الصادر عن جامعه الدول العربية في عام 2022 هذه التحديات ووصفها بالانفلات الرقمي حيث تمارس الرقابة الرقمية في ظل غياب رقابة قضائية صارمه واليات قانونيه تضمن المساءلة والشفافية كما اكدت تقرير على الحاجة الماسة لوضع عطر قانونيه وتشريعيه واضحة لحماية الخصوصية الرقمية ومنع التجاوزات التي تهدد الحريات الرقمية.

ثانيا: ضعف الاطر القانونية الدولية في مواجهه الرقابة الرقمية

ان غياب اطار قانوني دولي موحد وملزم ينظم الرقابة الرقمية او يجرم التجاوزات في هذا المجال يعتبر من التحديات الكبرى التي تواجه حمايه الحقوق الرقمية بشكل فعال على الرغم من وجود نصوص قانونيه دوليه عامه مثل المادة 17 من العهد الدولي للحقوق المدنية والسياسية لعام 1966 التي تكفل الحقه في الخصوصية وحمايه الافراد من التدخل غير المقنن في حياتهم الخاصة الى ان هذه النصوص تفتقر الى التفاصيل التقنية والإجرائية اللازمة لتنظيم المراقبة الحكومية في الفضاء الرقمي

[1]- انظر: كوثر حميدان، الخصوصية الرقمية في ظل تحديات الرقابة الإلكترونية، مجله الحقوق والعلوم السياسية، جامعه محمد خيضر، بسكرة، العدد 19، 2001 ص 97

[2]- انظر: مريم الشريف، مرجع سابق، ص 48

المعقد هذا العجز يشكل ثغره تتيح مجالا واسعا للدول لاستغلال الغموض القانوني وتبرير الممارسات المراقبة الشاملة بمبررات مثل الامن القومي او مكافحه الارهاب.[1]

في نفس السياق اوضحت الباحثة مريم شريف ان الإطار القانوني الدولي الحالي لا يتضمن معايير دقيقه ومحدده لتنظيمه الأنشطة الرقابية الرقمية مما يمنح الدول الفرصة التفسير النصوص القانونية بطريقه تخدم مصالحهم السياسية او الأمنية واشاره الى ان هذا الفراغ القانوني يساهم في تقليص الحق في الخصوصية الرقمية حيث يتم استغلال هذا الوضع من طرف بعض الدول لتبرير التدخلات الواسعة في الاتصالات الرقمية دون الخضوع لمعايير الدولية ملزمه.[2]

اضافه الى ذلك اكدت كوثر حميدان على محدودية الاليات الرقابية والمسائلة في القانون الدولي مشيره بذلك الى ان النظام القانوني الدولي لا يزال عاجزا عن تطوير ادوات فعاله لضبط التجاوزات الرقمية التي تقوم بها الدول. كما قامت بتوضيح ان غياب هذه الاليات يؤدي الى اضعاف الضمانات القانونية التي يفترض ان توفر الحماية للأفراد من الانتهاكات الرقمية مما يعزز من حاله انعدام الثقة واليقين بشأن حمايه الحقوق في البيئة الرقمية وعليه في الضمانات الدولية تبقى غير كافيه لمواجهه التحديات المتزايدة الناتجة عن الاستخدام المتزايد وعن المراقبة المستمرة. [3]

تجدر الإشارة ايضا الى ان الشبكة العربية للحقوق الرقمية اصدرت تقرير عام 2023 يبرز ان ممارسه المراقبة الرقمية في المنطقة العربية غالبا ما تنفذ دون رقابة قضائية فعاله وتتفاقم هذه المشكلة في خطورتها بسبب مشاركه القطاع الخاص في توفير تقنيات المراقبة مما يزيد من مخاطر استغلال هذه الادوات لانتهاك الحقوق الرقمية وكذلك اشار التقرير الى هذا الوضع فيما قد يسبب في تفاقم التحديات المتعلقة بالموازنة بين متطلبات الامن وضمان خصوصية. [4]

ثالثا: التأثير السلبي على الحقوق الرقمية الأخرى

تلحق الرقابة الرقمية التي تمارسها الحكومات انتهاكا غير مباشر لحقوق اساسيه مثل حريه التعبير والحق في الوصول للمعلومات وذلك من خلال ظاهره تعرف بتأثير التبريد الرقمي هذه الظاهرة تجعل الافراد يشعرون بالخوف من المراقبة المستمرة مما يدفعهم الى الامتناع عن التعبير بحريه عن

[1]- انظر: نفس المرجع، ص 49
[2]- كوثر حميدان، مرجع سابق، ص 101
[3]- الشبكة العربية لحقوق الانسان، الموازنة بين الامن الرقمي والخصوصية قراءة قانونية عربية، عمان، 2023، ص 12
[4]- انظر: اماني ابو الخير، الرقابة الرقمية وتأثيرها على حرية التعبير، مجلة الدراسات القانونية والدولية، جامعة القاهرة، العدد13، 2020، ص 124

آرائهم ووجهات نظرهم او التفاعل عبر المنصات الرقمية (1) كما ان اماني ابو الخير اوضحت في نفس السياق ان هذا الشعور بالخوف يقلل من الشفافية والمصداقية في النقاشات في البيئة الرقمية ويؤدي الى انتهاك حريه التعبير في الدول التي تدعي التزامها بحمايه هذه الحقوق.[1]

كما انه قد كشفت ابحاث اجراها مركز حرية الاعلام العربي في عام 2004 ان مخاوف المستخدمين من التعقب والتجسس الرقمي تدفعهم الى اعتماد وسائل حماية لهوياتهم مثل استخدام الادوات اخفاء الهوية او اللجوء الى منصات رقمية سرية لتجنب المراقبة. [2]

الفرع الثاني: الجرائم الالكترونية وتأثيرها على الافراد والمجتمعات

تشكل الجرائم الإلكترونية أحد أبرز التحديات التي فرضها التحول الرقمي، لما تنطوي عليه من تهديدات تمس الأفراد والمجتمعات على حد سواء. فهي لا تقتصر على الأضرار المادية، بل تمتد لتطال الخصوصية والأمن والاستقرار النفسي والاجتماعي. مما يجعل مكافحتها ضرورة لحماية القيم والمصالح في البيئة الرقمية.

أولا: تعدد اشكال الجرائم الإلكترونية واستهدافها للحقوق الأساسية

تعتبر الجرائم الإلكترونية تحديا خطيرا للحقوق الرقمية حيث تسبب انتهاكات متنوعة تستهدف الحقوق الأساسية المعترف بها دوليا حيث تعد الفضاءات الرقمية بخصبه للجرائم المتطورة والتي يقوم بارتكابها افراد وجماعات منظمه او حتى جهة حكومية وفي اغلب الاحيان تفلت من العقاب بسبب ضعف الاطر القانونية الدولية الخاصة بالبيئة الرقمية.

ومن أبرز هذه الجرائم:

1- الابتزاز الالكتروني: ويعتبر أكثر الجرائم شيوعا الذي يستخدم المجرمون معلومات او بيانات حساسة كالصور والبيانات الشخصية التي يكون قد تم الحصول عليها بطرق لا مشروعه ابتزاز الضحايا واجبارهم على دفع مبالغ ماليه او تقديم تنازلات مما يضعف الشعور بالأمان الشخصي ويخدش الكرامة الإنسانية.[3]

---

[1]- انظر: نفس المرجع، ص 127

[2]- انظر: ناصر احمد، الجرائم الإلكترونية وأثرها على الحق الخصوصية في القانون الدولي، مجله البحوث القانونية والسياسية، العدد 13، 2013، ص 147

[3]- انظر: يحيى عبد الرحمن، انتهاك الجرائم الإلكترونية للحق في الخصوصية من منظور القانون الدولي، مجله الفكر والقانون السياسي، مجلد 8، عدد 1، 2014 ص 379

2- الاختراق الالكتروني: تتبلور هذه الجريمة في الدخول غير المشروع الى الأنظمة والبيانات الخاصة بالأفراد او المؤسسات سواء كان ذلك بهدف سرقه المعلومات او التلاعب بها وهذا يشكل بوضوح انتهاك للحق في الخصوصية والسرية الرقمية.[1]

3- التحرش والتهديدات عبر الانترنت: يكون الاشخاص المستهدفون من هذه الجريمة اشخاصا ضمن الفئة الهشة من المجتمع كالنساء مثلا والاقليات مما يؤدي الى تقييد حريه التعبير والمشاركة والتفاعل في البيئة الرقمية احترازا من الايذاء النفسي او الاجتماعي.[2]

4- نشر خطاب الكراهية والاشاعات يعد هذا النوع من الجرائم اعتداء على الحق في التمتع ببيئة رقمية امنة ومحترمة فهذا الاخير يساهم في الزيادة من التوترات الاجتماعية وتهديد تماسك المجتمع.[3]

5- انتحال الهوية الرقمية في هذه الحالة يقوم المجرمون بسرقه الرقمية للأفراد والقيام بعملية احتيالية عن طريقها او لأغراض سياسية بما يلحقه اضرارا جسيما للضحايا.

هذه الجرائم لا تمس فقط الحق في الخصوصية بل تطال حتى حرية التعبير والحق في الحماية من العنف الرقمي والحق في التواصل والوصول الى المعلومات وقد أكد بعض الباحثين على ان مثل هذه الممارسات تفرض رقابة غير مباشره على سلوك وتصرفات الافراد في الفضاء الرقمي وتنشر ما يعرف بتأثير التخويف الذي يمنع المستخدمين من المشاركة في الأنشطة الرقمية بحرية.

ثانيا: ضعف الحماية القانونية الدولية للحقوق الرقمية في مواجهه الجرائم الإلكترونية

رغم الانتشار والتفاقم الطارئ على الجرائم الإلكترونية التي تستهدف الحقوق الرقمية الا ان النظم القانونية الدولية لا تزال تعاني من القصور الواضح في توفير الحماية القانونية الكافية لمواجهه هذه التهديدات ويرجع ذلك الى عوامل متعددة قانونيه وبنيويه تجعل من الصعب التصدي الفعال لهذه الجرائم على المستوى الدولي.

1- غياب اتفاقية دولية شاملة وملزمة: معنيه تحديدا بالحقوق الرقمية ما يتركوا فراغا تشريعيا تقوم بعض الدول باستغلاله لتمرير الانتهاكات تحت غطاء السيادة الوطنية او مكافحه الارهاب في الاتفاقيات

[1]- انظر: نفس المرجع، ص 379
[2]- انظر: نفس المرجع، ص 380

[3]- انظر: الخولي منى، الفراغ القانوني الدولي في مواجهه الجرائم الإلكترونية، مجله القانون الرقمي الدولي، جامعه دمشق، العدد 5، 2012، ص 63.

الحالية كالعهد الدولي الخاص بالحقوق المدنية والسياسية لم يتناول المسائل التقنية للفضاء السيبراني بشكل دقيق الامر الذي يضعف حماية الحقوق الرقمية.[1]

2- طبيعة الجرائم الإلكترونية العابرة للحدود:

حيث تشكل الطبيعة العابرة للحدود للجرائم الإلكترونية تحديا ثقيلا امام امكانيه المتابعة القضائية الدولية لا سيما في ظل الاختلافات بين الأنظمة القضائية الوطنية وغياب اليات التعاون القانوني فعاله وعمليه.

3- الاختلاف في التصور القانوني بين الأنظمة الدولية:

تعيق الفروق في القانونية بين الأنظمة الدولية بمفاهيم الخصوصية وحريه التعبير وحريه الوصول الى الانترنت امكانيه التوصل الى توافق بشأن خلق معايير او اتفاقيات دوليه موحده مما يلقي بمنظور سلبي على حماية الحقوق الرقمية وتعزيزها.[2]

علاوة على ذلك فان بعض المبادرات الدولية والإقليمية اتفاقيه بودابيست مثلا المرتبطة بالجرائم الإلكترونية رغم ثقلها واهميتها كإطار قانوني تم انتقادها لأنها صنعت في سياق اوروبي ولم تعطي وجهه نظر الدول النامية اهميه مما يجعله من تطبيقها على النطاق العالمي امرا معقدا.[3]

ثالثا: تأثير الجرائم الإلكترونية على ممارسه الحقوق الرقمية:

لا يقتصر تأثير الجرائم الإلكترونية على الحق في الخصوصية فقط بل تمتد الى اضعاف وتقليص مجموعه واسعه من الحقوق الرقمية الأساسية مثل الامن الرقمي وحريه التعبير فيلجا الافراد الى الحد من مشاركتهم وتفاعلهم عبر الانترنت خوفا من التعرض للاستهداف او الاختراق او التعقب في الفضاء الرقمي وهذا ما يؤدي الى تقليص ممارسه حقوقهم الرقمية بشكل عام ويشكل تهديدا خطيرا للحق في المشاركة الرقمية الحرة والأمنة.

الفرع الثالث: تأثير الشركات الكبرى على الحقوق الرقمية

شهد العالم خلال العقدين الاخيرين صعودا غير مسبوق لشركه التكنولوجيا الكبرى التي تسيطر على البنى التحتية للفضاء الرقمي وتتحكم في التدفقات المعلومات والمحتوى والبيانات عبر العالم وكمثال

---

[1]- انظر: عمر رنا، الاختلافات التشريعية الدولية بشأن حريه التعبير في الفضاء الرقمي، المجلة العربية للاعلام الالكتروني، في المجلد6، العدد 1، 2020،ص 49

[2]- انظر: ناصر احمد، مرجع سابق، ص 150

[3]- انظر: منظمه العفو الدولية: ميانمار، انظمة فيسبوك روجت العنف ضد روهينجا، تقرير منشور 2022/9/29، النسخة العربية، ص 1-2، الموقع amnesty.org/ar

على أبرز هذه الشركات نجد ميتا(Meta) جوجل (Google) تويتر (X) وهي شركات تعود في أصلها الى امريكا وتسيطر على أكثر من 80% من خدمات التواصل والبحث والاعلان الرقمي.

هذا الاحتكار لم يعد مجرد واقع اقتصادي بل تحول الى قوه مؤثره في حقوق الانسان الرقمية مما ادى الى بروز تحديات قانونيه تتعلق بالرقابة الخصوصية وحريه التعبير والسيادة الوطنية على الفضاء الرقمية وتعكس التجارب الدولية الحديثة هشاشه الإطار القانوني العالمي في ضبط هذه الهيمنة في ظل غياب المساءلة وضعف الضوابط التقنية والقانونية.

أولا: هيمنة الخوارزميات وتنقيح المحتوى

تعمل خوارزميات الشركات التقنية الكبرى مثل ميتا على تصفية وفلترة المحتوى وتحديد ما يظهر للمستخدمين مما يؤثر تأثيرا كبيرا على طبيعة المعلومات المتلقات من طرف الافراد ووفقا لتقرير منظمة العفو الدولية بعنوان ميانمار فان انظمه الفيس بوك روجت للعنف ضد الروهينغا حيث لم تقتصر خوارزميات المنصة على السماح لخطاب الكراهية ضد اقليه الروهينغا بالانتشار فقط بل عملت على تعزيز تفاعله ونشره الى نطاق اوسع من المستخدمين مما ادى الى تأجيج العنف الواقعي ضد هذه الفئة وهذا يبرز ان الخوارزميات ليست مجرد ادوات تقنيه محايده بل تتحول الى سبب محوري ورئيسي لنشر الكراهية مما يقلص حرية التعبير وحق المستخدمين في الوصول الى المعلومات دقيقة والصحيحة.[1]

ثانيا: استغلال الخصوصية كنموذج اعمال ربحي

تعتمد نماذج الاعمال الشركات التقنية الكبرى مثل ميتا على تحليل سلوك المستخدمين بشكل معين لتعزيز التفاعل وزيادة الارباح متجاوزتا بذلك مجرد كونها وسيله لعرض الاعلانات الى انتهاك الخصوصية من خلال استهداف اعلاني يعتمد على البيانات الحساسة دون موافقة صريحة او حقيقية من المستخدمين مما يتعارض مع المعايير الدولية المقربة لحماية البيانات الشخصية كما اشار تقرير منظمة العفو الدولية فان ميتا على الرغم من انها على علم بخطورة خطاب الكراهية الذي تروج له خوارزمياتها منذ 2012 الا انها لم تتخذ اجراءات كافية تحد منه وذلك تفضيلا للأرباح على حساب الخصوصية والامان الرقمية مشكلتا بذلك تهديد مباشر للحقوق الرقمية الأساسية.[2]

[1]-انظر: نفس المرجع

[2]- انظر مريم الشريف، اشكالية حرية التعبير في البيئة الرقمية، قراءة في السياسات شركات التكنولوجيا الكبرى، مجلة السياسة الدولية، العدد ،24، مركز الدراسات استراتيجية، القاهرة،2021، ص18

ثالثا: تهديد سيادة الدول واداره المحتوى

بحيث يشكل نفوذ المتزايد لشركات التكنولوجيا الكبرى مثل يوتيوب ومتى تهديدا مباشرا وواضحا للسيادة القانونية والتنظيمية للدول خاصه في الفضاء الرقمي فهذه الشركات تتحكم في المحتوى المنشور من خلال لوائح داخليه تفتقر الى الشفافية وتتخذ قرارات حذف او تقييد منشورات في المستخدمين دون اذن القضائي مما يقوض قدره الدولة على تنظيم فضائها الرقمي قوانينها الوطنية.

غالبا ما تزيل المنصات محتوى سياسي او اجتماعي حساس معتبرة في ذلك معايير خاصة دون توفير اليات وسبل واضحة لتفسير هذه القرارات او الاعتراض عنها كما انه قد اظهرت دراسات ان هذه الممارسات تعزز وتشجع تبعيه الدول لسياسات الشركات الأجنبية التي تمارس رقابة عابره للحدود مؤثرة بذلك سلبا على الديمقراطية وسيادة القانون.[1]

المطلب الثالث: امثلة عن قضايا دولية ذات صلة بالحقوق الرقمية

في ظل التوسع الهائل لاستخدام التكنولوجيا والفضاء الرقمي، أصبحت الحقوق الرقمية في قلب النقاشات القانونية والسياسية حول العالم. وقد برزت عدة قضايا دولية شهيرة سلطت الضوء على الانتهاكات التي قد تطال خصوصية الأفراد وحرية التعبير وسلامة البيانات. تشكّل هذه القضايا نماذج تطبيقية توضح التحديات المعاصرة التي تواجه حماية الحقوق الرقمية، وتبرز دور الاتفاقيات الدولية والقوانين الوطنية في التصدي لهذه الانتهاكات.

الفرع الأول: قضية توقيف القرصان الروماني "Guccifer" (مارسيل لازار) – 2014

"Guccifer"هو الاسم الحركي للقرصان الإلكتروني الروماني **مارسيل لازار لاهيل**(*MarcelLehelLazar*)،وهو موظف حكومي سابق في رومانيا تحول إلى هاكر فردي، برز اسمه عالميًا بعد قيامه باختراق حسابات شخصيات سياسية بارزة.

بين عامي 2012 و2014، قامGuccifer باختراق حسابات بريد إلكتروني خاصة لعدد من المسؤولين الأمريكيين والأوروبيين، ومنهم:

- وزيرة الخارجية الأمريكية السابقة هيلاري كلينتون.
- رئيس الولايات المتحدة السابق جورج بوش الأب.
- مستشارون في البيت الأبيض.

[1]- الموقع الرسمي لوزارة العدل الامريكية، الرابط:
https://www.justice.gov/archives/opa/pr/romanian-hacker-guccifer-sentenced-52-months-prison-computer-hacking-crimes

خلال تلك العمليات، كشفGuccifer عن مراسلات خاصة وسرية، وشاركها مع وسائل الإعلام، ما أثار فضيحة سياسية كبيرة داخل الولايات المتحدة وعند توقيفGuccifer من قبل السلطات الرومانية، تقدّمت الولايات المتحدة **بطلب رسمي لتسليمه** بموجب اتفاقية بودابست، التي صادقت عليها كل من رومانيا والولايات المتحدة ونظراً لتصنيف الاختراق والقرصنة ضمن الجرائم الإلكترونية المنصوص عليها في الاتفاقية، ووجود **تشريعات متقاربة** بين البلدين، وافقت رومانيا على طلب التسليم.

في **أبريل 2016**، وافقت رومانيا على تسليمGuccifer إلى السلطات الأمريكيةحيث مثل أمام محكمة فدرالية في فرجينيا، **وأقرّ بالجريمة** في اختراق البريد الإلكتروني وسرقة هوية.

حكم عليه بالسجن لمدة **52شهرًا (4 سنوات و4 أشهر)** في الولايات المتحدة.

أثبتت القضية **فعالية اتفاقية بودابست كأداة قانونية للتعاون الدولي** في ملاحقة الجرائم الإلكترونية عبر الحدود كما أظهرت كيف يمكن **للتنسيق القضائي** أن ينجح في تجاوز تعقيدات السيادة القضائية، خاصة في الجرائم العابرة للحدود.[1]

الفرع الثاني: قضية Facebook–Cambridge Analytica

تمثّل قضيةFacebook–Cambridge Analytica واحدة من أخطر فضائح الخصوصية الرقمية في القرن الحادي والعشرين، وقد كشفت عن هشاشة النظم القانونية المتعلقة بحماية البيانات الشخصية أمام طموحات الشركات التجارية والسياسية. هذه القضية لم تكن مجرد حادث تقني، بل مثّلت نقطة تحول عالمية في فهم وتفعيل القوانين الدولية، وعلى رأسها **اللائحة العامة لحمايةالبيانات (GDPR)**الصادرة عن الاتحاد الأوروبي، كما أثّرت في توجهات تشريعية على مستوى عالمي.

في مارس 2018، نشرت صحيفتا The Guardian البريطانية و The New York Times الأمريكية تقارير موسّعة كشفت أن شركة تحليل البيانات البريطانية Cambridge Analytica جمعت بشكل غير قانوني معلومات عن أكثر من87 مليون مستخدم لفيسبوك .هذه البيانات استخدمت في التأثير على نتائج الانتخابات، وعلى رأسها:

- الانتخابات الأمريكية2016، لدعم حملة دونالد ترامب.
- استفتاء خروج بريطانيا من الاتحاد الأوروبي(Brexit) عام 2016.[2]

[1]- انظر موقع صحيفة غارديان،الرابط:
https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.com

[2]- انظر: نفس المرجع

البيانات لم تُجمع مباشرة من قبل الشركة، بل عبر تطبيق إلكتروني أنشأه باحث أكاديمي يُدعى ألكسندر كوغان، بعنوان .This Is Your Digital Life :هذا التطبيق طلب من المستخدمين السماح بالوصول إلى معلوماتهم لأغراض بحثية، لكنه في الواقع جمع أيضًا بيانات أصدقائهم دون علمهم أو موافقتهم.

"في تلك الفترة، لم تكن فيسبوك تُقيّد وصول تطبيقات الطرف الثالث إلى بيانات المستخدمين وأصدقائهم، مما جعل التسريب ممكنًا".

تشير فحوى القضية إلى عدد من الانتهاكات الجوهرية التي تتناقض مع القوانين الوطنية والدولية المعنية بحماية البيانات، نذكر من بينها:

لم يحصل المستخدمون ولا أصدقاؤهم على إشعار بأن بياناتهم ستُمنح لأطراف ثالثة، مما يُعد **خرقًا مباشرًا لحق الموافقة**، الذي تُقرّه المادة 6 من **اللائحة العامة لحماية البيانات.GDPR**

لم يكن مستخدمو فيسبوك على علم بأن تطبيقًا ترفيهيًا بسيطًا سيؤدي إلى استخدام معلوماتهم في أغراض انتخابية. وهذا ينتهك المادة 12 من GDPR بشأن "حق الشخص في أن يتم إعلامه بطريقة واضحة ومفهومة حول استخدام بياناته."

جمعت البيانات بحجة "بحث علمي"، لكنها استُخدمت **في استهداف سياسي وإعلانات موجهة**، ما يُعد خرقًا لمبدأ تحديد الغرض (Purpose Limitation) المنصوص عليه في المادة 5 من GDPR.

"شكلت القضية ضربة قوية لمصداقية فيسبوك، ودفعت إلى تحقيقات قانونية في أكثر من 20 دولة".

رغم أن الانتهاكات وقعت قبل تفعيل GDPR في مايو 2018، إلا أن القضية كانت **دافعًا مباشرًالتطبيق صارم** لأحكام اللائحة في القضايا التالية، ودفعت البرلمان الأوروبي إلى**استدعاء ماركزوكربيرغ للشهادة** أمام لجانه.

مثّلت الفضيحة تجسيدًا حيًّا لأهميةGDPR، فأظهرت الحاجة لقواعد قانونية قوية تحكم كيفية جمع ومعالجة ونقل البيانات الشخصية، حتى من قبل شركات عابرة للقارات.

- شجّعت القضية على تطوير قوانين محلية مشابهة، مثل:

قانون حماية البيانات في البرازيل.(LGPD) و مشروع قانون الخصوصية في الهند.(DPDP)

وقانون الخصوصية الأمريكي المقترح.(ADPPA)

- أدى الحادث إلى إطلاق حملة عالمية بعنوان .#DeleteFacebook
- بدأ الملايين من المستخدمين بمراجعة إعدادات الخصوصية الخاصة بهم، وأصبحت مفاهيم مثل "الحق في المعرفة" و"الحق في المحو" أكثر تداولًا[1].

على الصعيد القانوني، واجهت شركة فيسبوك عقوبات مالية ضخمة من جهات تنظيمية في كل من الولايات المتحدة والمملكة المتحدة، نتيجة لانتهاكها الصارخ لخصوصية المستخدمين. ففي عام 2019، فرضت **لجنة التجارة الفيدرالية الأمريكية(FTC)** غرامة قياسية على فيسبوك بلغت **5 مليارات دولارأمريكي،** في واحدة من أكبر العقوبات في تاريخ قضايا الخصوصية، وذلك بسبب مخالفتها لالتزامات سابقة تتعلق بحماية بيانات المستخدمين. [2]

أما في **المملكة المتحدة،** فقد قررت **هيئة حماية البيانات(ICO)** تغريم الشركة مبلغ **500ألف جنيه إسترليني،** وهو الحد الأقصى المسموح به حينذاك بموجب القانون البريطاني، على خلفية خرق فيسبوك لقواعد حماية البيانات الوطنية وعدم التزامها بمبدأ الشفافية في جمع المعلومات الشخصية.[3]

[1]- انظر: الموقع الرسمي لقناة(CBS)، الرابط-https://www.cbsnews.com/news/deletefacebook trends-amid-cambridge-analytica-scandal/?utm.com

[2]- انظر: الموقع الرسمي **لجنة التجارة الفيدرالية الأمريكية،الرابط:** https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-facebook

[3]- انظر: الموقع الرسمي لهيئة حماية البيانات،الرابط: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-/fined-500-000

الخاتمـــة

الخاتمة:

بعد التطرق إلى الإطارين المفاهيمي والقانوني للحقوق الرقمية، وتحليل أبرز الاتفاقيات الدولية ذات الصلة، واستعراض الجهود المبذولة لمواجهة التحديات الراهنة التي تهدد هذه الحقوق في البيئة الرقمية، يمكن القول إن الحقوق الرقمية باتت تمثّل أحد المحاور الجوهرية في منظومة حقوق الإنسان المعاصرة، لما لها من صلة مباشرة بحياة الأفراد وحرياتهم في الفضاء الإلكتروني. وقد كشفت هذه الدراسة عن مدى الحاجة إلى فهم دقيق لطبيعة هذه الحقوق، وتأطيرها قانونيًا على نحو يستجيب للتطور التكنولوجي المستمر، ويحمي الإنسان من الانتهاكات التي قد يتعرض لها في هذا المجال.

من خلال دراستنا للحقوق الرقمية على المستوى الدولي، أمكننا التوصل إلى جملة من النتائج المهمة التي تسلط الضوء على واقع هذه الحقوق في ظل التقدم التكنولوجي المتسارع، وسعي المجتمع الدولي لتوفير الحماية القانونية الكافية لها.

أولًا، تبيّن أن الاتفاقيات الدولية لحقوق الإنسان، وعلى رأسها الإعلان العالمي والعهد الدولي، قد أولت عناية واضحة للحقوق الرقمية، ولو بصفة غير مباشرة، من خلال نصوصها ذات الصياغة العامة والمرنة. هذه الصياغات أتاحت إمكانية تفسير الحقوق التقليدية على نحو يشمل مظاهرها الرقمية، مثل حرية التعبير عبر الوسائط الإلكترونية، وحق حماية الحياة الخاصة والبيانات الشخصية، وكذا الحق في النفاذ إلى المعلومات وتداولها.

ثانيًا، تأكد أن المجتمع الدولي شرع في اعتماد أطر قانونية خاصة تتعلق بالحقوق الرقمية، تمثلت في عدد من الاتفاقيات المتخصصة، من أبرزها اتفاقية بودابست لمكافحة الجريمة الإلكترونية، التي تعد أول اتفاقية دولية تعالج الجرائم المعلوماتية. إلى جانب ذلك، ظهرت مبادرات تنظيمية إقليمية متقدمة، أهمها اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي، والتي تُعد من النماذج الرائدة في مجال حماية البيانات والخصوصية الرقمية، بما تحتويه من مبادئ ومعايير صارمة وشفافة.

ثالثًا، وعلى الرغم من هذه الخطوات الإيجابية، إلا أن الحقوق الرقمية لا تزال تواجه تحديات متزايدة، من أبرزها ضعف التنسيق القانوني على المستوى الدولي، وتفاوت مستوى الحماية بين الدول، إضافة إلى تزايد ممارسات الرقابة والتجسس الرقمي من قبل بعض الحكومات، واتساع نطاق الجرائم الإلكترونية، ما يؤدي إلى إضعاف فعالية الحماية القانونية، ويُهدد الحقوق الرقمية في أكثر من سياق جغرافي وسياسي.

رابعًا وأخيرًا، أظهرت العديد من القضايا الدولية المعاصرة الفجوة القائمة بين تسارع الابتكار التكنولوجي من جهة، وقدرة التشريعات الوطنية والدولية على مجاراته من جهة أخرى .وهو ما يفرض مراجعة مستمرة للأطر القانونية القائمة، وتفعيل آليات التعاون الدولي في مجال الأمن السيبراني، إلى

جانب نشر ثقافة الحقوق الرقمية لدى مختلف الفاعلين، سواء على مستوى الأفراد أو المؤسسات، لضمان استخدام آمن ومسؤول للتكنولوجيا.

فرغم التقدّم الملحوظ في بلورة مفهوم الحقوق الرقمية على المستوى النظري، سواء من خلال الدراسات القانونية أو المبادرات الأممية، فإن الواقع العملي يكشف عن فجوة مقلقة بين هذا الإطار النظري المتقدم وبين التطبيق الفعلي في ظل الظروف الدولية الراهنة. فالكثير من الدول والمؤسسات لا تزال تتعامل مع الفضاء الرقمي كمنطقة رمادية قانونيًا، ما يجعل الحقوق المرتبطة به عرضة لانتهاكات مستمرة.
لقد أوضحت الأحداث الدولية الأخيرة، مثل التسريبات المتعلقة بالمراقبة الجماعية، وانتشار برامج التجسس، وتنامي هيمنة الشركات التكنولوجية، أن الحماية القانونية للحقوق الرقمية لم ترقَ بعد إلى مستوى التحديات التقنية والأمنية والاجتماعية التي تفرضها البيئة الرقمية الحديثة. كما أن ضعف الالتزام الدولي، وغياب آليات فعالة للرصد والمساءلة، يعمّق من هشاشة هذه الحقوق ويزيد من التفاوت الرقمي بين الدول والأفراد.

وفي ظل هذا الوضع، فإن ترسيخ الحقوق الرقمية كحقوق إنسانية فعلية، لا يمكن أن يتحقق إلا عبر سدّ هذه الفجوة القانونية والمؤسساتية. ومن أجل ذلك، يوصى بالعمل على:

1- **وضع إطار قانوني دولي ملزم** يعترف صراحة بالحقوق الرقمية كجزء من منظومة حقوق الإنسان، ويحد من استخدام الفضاء الرقمي كأداة للرقابة أو القمع.
2- **اعتماد اتفاقية دولية موحّدة لحماية البيانات الشخصية**، على غرار اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، تكون مرجعية شاملة لجميع الدول وتُراعي العدالة الرقمية.
3- **تفعيل آليات الرصد والمساءلة على المستوى الأممي**، وتوسيع صلاحيات الهيئات المختصة بمراقبة انتهاكات الحقوق الرقمية، لضمان شفافية أكبر ومحاسبة الجهات المنتهكة، سواء كانت دولًا أو شركات.
4- **سنّ تشريعات وطنية تتماشى مع المعايير الدولية** وتتكيف مع تطور التكنولوجيات الحديثة، من خلال نصوص واضحة تضمن حماية الخصوصية، حرية التعبير، وأمن المستخدمين في البيئة الرقمية.
5- **تعزيز التعاون الدولي في مكافحة الجرائم السيبرانية** وتبادل المعلومات التقنية والقانونية، بهدف التصدي للمخاطر العابرة للحدود التي تهدد الأمن الرقمي العالمي.
6- **إدماج التربية الرقمية ضمن السياسات الوطنية والتعليمية**، بما يُمكّن الأفراد من الوعي بحقوقهم الرقمية ويمدّهم بالمعرفة القانونية والتقنية الضرورية للدفاع عنها.

إنّ هذه التوصيات تمثّل خطوات ضرورية لسدّ الهوّة القائمة بين المبادئ النظرية والتطبيق الفعلي، وتُعدّ مدخلًا حيويًا لبناء نظام قانوني رقمي عادل، يضمن احترام الحقوق الرقمية وكرامة الإنسان في زمن العولمة الرقمية.

قائمة المراجع

قائمة المراجع

المصادر

- الإعلان العالمي لحقوق الانسان 1948
- العهد الدولي الخاص بالحقوق المدنية والسياسية 1966
- اتفاقية بودابست 2001
- اللائحة العامة لحماية البيانات(GDPR) 2018

كتب

- هاني سليمان، حقوق الإنسان وحريات الأساسية، دار الشروق للنشر والتوزيع، عمان، 2000
- علي وهبي، الحق في حماية البيانات الشخصية، بيروت، منشورات الحلبي الحقوقية، 2003
- إسماعيل عبد الفتاح عبد الكافي، حقوق الانسان العامة في الإسلام (د ب ن) ،2006
- انظر: الحمادي طارق، الجرائم الإلكترونية في القانون الدولي والوطني: دراسة مقارنة، دار الجامعة الجديدة للنشر، القاهرة، 2009
- أحمد أبو الوفاء، الوسيط في القانون الدولي العام، دار النهضة العربية للنشر والتوزيع، طبعة 4، 2010
- نجلاء أحمد ياسين، الرقمنة وتقنياتها في المكتبات العربية، العربي للنشر والتوزيع، القاهرة 2012
- محمد الطاهر، الحرية الرقمية، المفاهيم الأساسية، مؤسسة حرية الراي والتعبير، ط 1، القاهرة، 2013
- مروة زين العابدين، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي والقانون الاتفاقي الوطني، القاهرة مركز الدراسات العربية للنشر والتوزيع، ط1، 2016.
- انظر: أحمد عبد الحفيظ الحسيني، الحق في حرية الرأي والتعبير في القانون الدولي لحقوق الإنسان، دار النهضة العربية، القاهرة، 2016
- محمد عبد العزيز عبد المنعم، حرية التعبير في العصر الرقمي: الضوابط والقيود في القانون الدولي، المركز القومي للبحوث الجنائية والاجتماعية، القاهرة، 2017.
- انظر خالد العربي، حقوق الإنسان في المواثيق الدولية والواقع العربي، دار الشروق، القاهرة، 2018
- بلال جعفر، الامن السبراني و حماية البيانات الشخصية،دار الخلدونية، الجزائر،2020
- محمد العيساوي،حرية التعبير في البيئة الرقمية: دراسة تحليلة قانونية، دار الهدى القاهرة،2020
- فتحي الفاضلي، *الحقوق الرقمية في ظل المجتمع الرقمي*، دار النشر الجامعية، تونس، 2021،
- بوعافية عبد الكريم، الحقوق الرقمية في البيئة الافتراضية، دراسة قانونية ، دار المعرفة ، الجزائر 2021

- نصر الله خالد، الرقابة وحرية التعبير في العالم العربي، الشبكة العربية لمعلومات حقوق الانسان، بيروت، 2021

- هالة أبو الحسن، القانون والتكنولوجيا: حماية البيانات الشخصية في البيئة الرقمية، دار النهضة العربية، القاهرة، 2021

رسائل جامعية

- وسام نعمت إبراهيم السعدي، الحقوق الرقمية وآليات الحماية المقررة لها في إطار القانون الدولي لحقوق الإنسان، كلية الحقوق، جامعة الموصل

- مريم الشريف، الخصوصية الرقمية في ظل القانون الدولي لحقوق الانسان، مذكره ماستر، جامعه سطيف 2022

مجلات

- كوثر حميدان، الخصوصية الرقمية في ظل تحديات الرقابة الإلكترونية، مجله الحقوق والعلوم السياسية، جامعه محمد خيضر، بسكرة، العدد 19، 2001

- الخولي منى، الفراغ القانوني الدولي في مواجهه الجرائم الإلكترونية، مجله القانون الرقمي الدولي، جامعه دمشق، العدد 5، 2012

- ناصر احمد، الجرائم الإلكترونية وأثرها على الحق الخصوصية في القانون الدولي، مجله البحوث القانونية والسياسية، العدد 13، 2013

- يحيى عبد الرحمن، انتهاك الجرائم الإلكترونية للحق في الخصوصية من منظور القانون الدولي، مجله الفكر والقانون السياسي، مجلد 8، عدد 1، 2014

- انظر: لونيسي علي، دور الإعلان العالمي لحقوق الانسان في إقرار الضمانات القضائية لحقوق الانسان، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ،المجلد 04، العدد 02

- اماني ابو الخير، الرقابة الرقمية وتأثيرها على حرية التعبير، مجلة الدراسات القانونية والدولية، جامعة القاهرة، العدد13، 2020

- عمر رنا، الاختلافات التشريعية الدولية بشأن حريه التعبير في الفضاء الرقمي، المجلة العربية للاعلام الالكتروني، في المجلد6، العدد 1، 2020،ص 49

- انظر: هشام شنيتي، الحقوق الرقمية بين القانون الدولي والواقع السيبراني، مجلة القانون والسياسة، جامعة الرباط، المغرب، العدد 6، 2022

- محمد حسن و عماد مكاوي، الخصوصية الرقمية في القانون الدولي و المواثيق الدولية، مجلة البحوث و الدراسات الإعلامية، العدد22، 2022

- احمد الشهري، "حرية التعبير و حدودها القانونية في البيئة الرقمية"، المجلة القانونية الجزائرية، العدد 44،2022

- غزيل عائشة، الحماية الدولية للحق في الخصوصية في المجال الرقمي، جامعة غليزان، مجلة المعيار، مجلد 27، العدد 04، 2022

مواقع الكترونية

- لجنة حقوق الانسان للأمم المتحدة، التعليق العام رقم 39 بشأن المادة 19 من العهد الدولي الخاص بالحقوق المدنية و السياسية،2011

- مجلس حقوق الإنسان التابع للأمم المتحدة(2012) ، /لقرار 8/20: تعزيز وحماية والتمتع بحقوق الإنسان على الإنترنت الأمم المتحدة

- الاتحاد الدولي للاتصالات فهم الامن السيبراني في المجتمع الرقمي 2013، متاح على الموقع: /https://www.itu.int/itu-d/sites/cybersecurity/ar

- المفوضية السامية لحقوق الانسان، "الحق في الخصوصية في العصر الرقمي "، الأمم المتحدة الدورة 39 لمجلس حقوق الانسان، الوثيقة رقم HRC/39/29/أوت 2018، ص5

- المفوضية السامية لحقوق الانسان، تقرير حرية التعبير،2019، جنيف، متاح على الرابط: https://www.ohchr.org/ar/freedom-of-expression

- هيئة الاتصالات والفضاءات التقنية CST، مركز المعرفة الرقمية البيانات الشخصية، الرابط: https://www.cst.gov.sa/ar/media-center

- مجلس حقوق الانسان الدورة 44، 2020

- اللجنة الأوروبية للحقوق الرقمية: دليل الامن السيبراني وحقوق الانسان، بروكسل، 2020

- اليونيسكو، حرية التعبير ووسائل الاعلام الرقمية، باريس 2021

- الامم المتحدة: الجمعية العامة، تعزيز الامن السيبراني وحماية حقوق الانسان، وثيقة 2021 A/76/136 ،متاح على الموقع: https://digitallibrary.un.org/?ln=ar

- منظمه العفو الدولية: ميانمار، انظمة فيسبوك روجت العنف ضد روهينجا، تقرير منشور 2022/9/29، النسخة العربية، ص 1-2، الموقع amnesty.org/ar

- معهد البحرين للتنمية السياسية، الموقع الرسمي،الرابط: https://www.bipd.org/publications/Articles/87753.aspx

- نص اتفاقية بوداباست ، تاريخ التصفح، متاح على الموقع : https://www.coe.int/en/web/cybercrime/the-budapest-convention

- الموقع الرسمي،اللائحة العامة لحماية البيانات، الرابط:https://gdpr-info.eu

-الموقع الرسمي، الهيئة العامة للأسماء والأرقام المخصصة على الإنترنت، الرابط:
https://www.icann.org/resources/pages/what-2012-02-25-en
- الموقع الرسمي، منظمة المنظمة الدولية للمعايير ،الرابط: https://www.iso.org/isoiec-27001-information-security.html :
- الموقع الرسمي، منتدى حوكمة الإنترنت، الرابط:
https://www.intgovforum.org/en/about
- الموقع الرسمي لوزارة العدل الامريكية، الرابط:
https://www.justice.gov/archives/opa/pr/romanian-hacker-guccifer-sentenced-52-months-prison-computer-hacking-crimes
- موقع صحيفة غارديان،الرابط:
https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.com
- الموقع الرسمي لقناة(CBS)،
الرابط-https://www.cbsnews.com/news/deletefacebook-trends-amid-cambridge-analytica-scandal.com
- الموقع الرسمي لجنة التجارة الفيدرالية الأمريكية،الرابط:
https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-facebook
- الموقع الرسمي لهيئة حماية البيانات،الرابط:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-fined-500-000

الفهـــــرس

الفهرس

شكر

إهداء

مقدمة: 1

الفصل الأول: الإطار المفاهيمي للحقوق الرقمية 5

المبحث الأول: مفهوم الحقوق الرقمية..... 6

المطلب الأول: تعريف الحقوق الرقمية 6

الفرع الأول: تعريف الحق لغة واصطلاحا 6

الفرع الثاني: تعريف الحقوق الرقمية..... 9

المطلب الثاني: خصائص الحقوق الرقمية..... 9

الفرع الأول: ارتباط التمتع بالحقوق الرقمية بالإقرار القانوني لها 10

الفرع الثاني: الطابع العالمي والمتطور لهذه للحقوق الرقمية 11

الفرع الثالث: الحقوق الرقمية حقوقا أساسية داعمة لحقوق الانسان 12

المطلب الثالث: التمييز بين الحقوق الرقمية والحقوق التقليدية..... 13

الفرع الأول :الوسيط في ممارسة الحق 13

الفرع الثاني :نطاق ممارسة الحق 13

الفرع الثالث: من حيث طبيعة الانتهاكات وطرق الحماية..... 14

المبحث الثاني: انواع الحقوق الرقمية 16

المطلب الأول: الحق في حرية التعبير الرقمية 16

الفرع الأول: تعريف الحق في حرية التعبير الرقمية..... 16

الفرع الثاني: الحق في التعبير عبر الفضاء الرقمي 17

الفرع الثالث: الخصائص المميزة لحرية التعبير عبر الانترنت..... 18

الفرع الرابع: حدود حرية التعبير في البيئة الرقمية 19

المطلب الثاني : الحق في الخصوصية وحماية البيانات 21
الفرع الأول: تعريف الحق في الخصوصية في الفضاء الرقمي 21
الفرع الثاني: محل الخصوصية الرقمية 23
الفرع الثالث: العلاقة بين الحق في الخصوصية الرقمية وبقية الحقوق الرقمية 25
المطلب الرابع: الامن السبراني من اجراء وقائي لضمان الحقوق الرقمية الى حق قائم بذاته 30
الفرع الأول: المفهوم العام للأمن السبراني: 30
الفرع الثاني: طبيعة الحق في الامن السبراني 31
الفرع الثالث: أبعاد الامن السبراني في مختلف المجالات 33
الفصل الثاني: الإطار القانوني للحقوق الرقمية على المستوى الدولي 36
المبحث الأول: الاتفاقيات واللوائح الدولية الدولية ذات الصلة 37
المطلب الأول: الشرعة الدولية لحقوق الانسان 37
الفرع الأول: استغراق مواد الإعلان العالمي لحقوق الإنسان للحقوق الرقمية 37
الفرع الثاني: استغراق مواد العهد الدولي الخاص بالحقوق المدنية والسياسية للحقوق الرقمية 41
المطلب الثاني: الصكوك الدولية الخاصة بالحقوق الرقمية 46
الفرع الاول: اتفاقية بودابست 46
الفرع الثاني: اللائحة العامة لحماية البيانات GDPR 50
المبحث الثاني: الجهود الدولية المبذولة لحماية الحقوق الرقمية في ظل التحديات الراهنة 56
المطلب الأول: الجهود الدولية المبذولة في حماية الحقوق الرقمية 56
الفرع الأول: اعتراف الأمم المتحدة بالحقوق الرقمية 56
الفرع الثاني: جهود المنظمات الدولية التقنية والتنظيمية 57
المطلب الثاني: التحديات التي تواجه اعمال الحقوق الرقمية 58
الفرع الأول: المراقبة الحكومية والتجسس الرقمي 58
الفرع الثاني: الجرائم الالكترونية وتأثيرها على الافراد والمجتمعات 61
الفرع الثالث: تأثير الشركات الكبرى على الحقوق الرقمية 63

المطلب الثالث: امثلة عن قضايا دولية ذات صلة بالحقوق الرقمية 65
الفرع الأول: قضية توقيف القرصان الروماني "Guccifer" (مارسيل لازار) – 2014 65
الفرع الثاني: قضيةFacebook–Cambridge Analytica 66
الخاتمة: 70
قائمة المراجع 74
الفهرس 79