
**الجامعة العربية الأمريكية**

**كلية الدراسات العليا**

# الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني ومن منظور المعايير الدولية "دراسة مقارنة"

إعداد

**ميس حمزة خالد عبد العزيز**

إشراف

**الدكتور رزق سمودي**

**تم تقديم هذه الرسالة استكمالاً لمتطلبات درجة الماجستير**

**في تخصص العلوم الجنائية**

**2025/ 3**

**إجازة الرسالة**

**الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني ومن منظور المعايير الدولية "دراسة مقارنة"**

إعداد

**ميس حمزة خالد عبد العزيز**

نوقشت هذه الرسالة بتاريخ 03/05/ 2025 وأُجيزت.

| أعضاء لجنة المناقشة: | | التوقيع |
|---|---|---|
| 1.د. رزق سمودي | مشرفا ورئيسا | ..... |
| 2.د. أحمد الأشقر | ممتحناً داخلياً | ..... |
| 3.د. أحمد بشتاوي | ممتحناً خارجياً | ..... |

## الإقرار

أقر بأن هذه الرسالة هي نسخة أصيلة لإنتاجي البحثي ولم يُقدم من قبلي لنيل أي درجة علمية لدى أي مؤسسة تعليمية أخرى، وقد تمت الإشارة إلى جميع المصادر والمراجع ذات العلاقة التي تم استخدامها.

اسم الطالبة : ميس حمزة خالد عبد العزيز

الرقم الجامعي: 20200218

التوقيع: 

التاريخ: 2025/07/08م

## الإهداء

إلى غزة هاشم وجنين القسام .

إلى الشهداء الأكرم منا جميعاً.

إلى من علّماني الثبات على المبدأ ، والإصرار على التقدم والنجاح ، والدي الحبيب وأمي الغالية.

إلى من ساندوني دوماً ، أشقائي الأعزاء

إلى الداعم الأول أختي الحبيبة.

إلى أمل الحياة أبنائي الأحبة جبران ورازي ويعرب .

ميس حمزة خالد عبد العزيز

## الشكر والتقدير

أتقدم بخالص الشكر والعرفان لأستاذي الفاضل، الدكتور رزق سمودي ، لقبوله الإشراف على رسالتي، وعلى ما بذله من جهد في الإشراف على هذه الرسالة .
كما أتقدم بالشكر الجزيل لأعضاء لجنة المناقشة الموقرة ،على تفضلهم بالموافقة على مناقشة هذه الرسالة.

ميس حمزة خالد عبد العزيز

# ملخص الرسالة

تهتم هذه الدراسة بالخصوصية في الفضاء الرقمي، وواقع حمايتها في ظل القوانين الدولية لحماية الخصوصية والبيانات الشخصية ، من خلال تحليل واستقراء العديد من النصوص الدستورية والجنائية والتشريعات المقارنة في هذا المجال ، إذ أنه في ظل تزايد حجم البيانات الشخصية التي يتم جمعها وتحليلها من قبل الشركات والحكومات في البيئة الرقمية ، أصبح استهدافها يثير مخاوفاً حول مدى احترام خصوصية الأفراد ، كما وتهدف الدراسة إلى تحليل الإشكالية القانونية التي تنشأ عن التعارض بين حق الأفراد الخصوصية الرقمية ، والحق في التحكم بالبيانات الشخصية من قبل الشركات والحكومات ، والتحدي القائم حول مدى تحقيق التوازن بين حماية الخصوصية الرقمية للأفراد وبين الحق المشروع للشركات في استخدام هذه البيانات الخاصة بالأفراد .

وقد تطرقت هذه الدراسة إلى نشأة مفهوم الخصوصية حتى تطورها في ظل وجود وسائل التكنولوجيا الحديثة والاتصالات.

وتناقش الرسالة أيضا الاتفاقيات والمعايير والمبادئ التوجيهية التي لها الدور الأساسي في الرقابة على التشريعات المتعلقة بالخصوصية في العصر الرقمي.

كما وتوصلت الدراسة إلى مجموعة من النتائج الرئيسية ، من أهمها أن حماية الحق في الخصوصية في العصر الرقمي هو مسؤولية مشتركة من عدة أطراف، وأن الحق في الخصوصية هو أساس ممارسة باقي الحقوق والحريات ، كما أن على المشرع الفلسطيني ضمان حماية هذا الحق وضمان حماية خصوصية الأفراد، وإقرار قانون خاص لحماية حق الخصوصية الرقمية في فلسطين.

الكلمات المفتاحية: الحق في الخصوصية، الخصوصية الرقمية، البيانات الشخصية، الذكاء الاصطناعي، المعايير الدولية، الحماية الجزائية للحق في الخصوصية الرقمية.

## فهرس المحتويات

## مقدمة

إن الحق في الخصوصية هو حق أساسي من حقوق الإنسان ، و مما لاشك فيه أن الحياة الخاصة للأفراد في الوقت الحالي تحتاج إلى حماية كبيرة، خاصةً بعد الانتهاكات التي تمس الحياة الخاصة من خلال التعدي الحاصل عليها من قبل الغير.

وللأهمية البالغة لحق الخصوصية في حياة الإنسان فقد تم السعي لوضع أسس ثابتة تمثل سياجاً منيعاً لحماية هذا الحق ، لما يعد ضمن نطاق الحق في الخصوصية وما يخرج عنه، مكتشفين الصعوبة البالغة في ذلك الأمر، حيث تبرز مشكلة تحديد الحق في الخصوصية وتطوراتها كإشكالية بحثية يتم تناولها من خلال عدة زوايا اجتماعية وقانونية وعدة اتجاهات أخرى.

هذا ويعيش العالم اليوم عصر الثورة المعلوماتية ،من حيث السرعة واليسر في نقل المعلومات وأداء المعاملات عبر الفضاء الرقمي ، ومما لا شك بأن كل تطور تقني له انعكاساته على المستوى القانوني ، إذ أن مسألة التطورات التكنولوجية أضحت مسألة تثيرالايجابيات وما يتبعها من آثار سلبية على بعض المصالح والحقوق التي تحتاج إلى الحماية الجزائية لها، سواء في إطار النصوص التقليدية أو باستحداث نصوص متوائمة مع طبيعتها والدور التي تؤديه في مختلف المجالات.

ونظراً لتغير معطيات العصر فقد تغيرت جميع النظم ، ومع التقدم العلمي والتكنولوجي المعاصر،برزت أساليب إجرامية بتقنيات حديثة أثرت بشكل كبير على مسألة الحق في الخصوصية في العصر الرقمي ، وقد زاد من التعقيد في مجال الحق في الخصوصية ، وذلك من خلال استخدام الوسائل الحديثة من قبل الأفراد أو الدولة ، فقد أصبح المستخدم معرضاً للاعتداء على حياته الخاصة، إذ أصبح من الصعب وفي الآونة الأخيرة حصر الجهات التي تقوم بجمع المعلومات الخاصة، وضرورة التوفيق بين أهمية نظم المعلومات الخاصة وبين عدم التعدي على حياة الأفراد الخاصة عند استخدام هذه النظم، حيث أن استعمالها أصبح أمراً لا مفر منه ، مما يجعل تدخل رجال القانون في البحث عن الحماية القانونية للحياة الخاصة أمراً ضروريا، سواء بتعديل القوانين الحالية أو من خلال اقتراح وتشريع قوانين جديدة حالة عدم استيعاب القوانين الجديدة ، وما استجد من مشاكل قانونية ، فلقد فرضت الثورة الرقمية بأبعادها التكنولوجية المختلفة العديد من التحديات في جميع المجالات ، وتأتي التحديات القانونية في مقدمة هذه التحديات من خلال تداول البيانات واستخدامها في العديد من المجالات ، والتي تجعلها لاتتلاءم ومعطيات الثورة الرقمية ، مما يفرض تطوير هذه النظم القانونية لتلائم هذه المعطيات الحديثة ،مما يجعل الحق في الخصوصية بمفهومه التقليدي ، وفي ظل النظم القانونية من أبرز التحديات ، إذا أن تطبيقات

العصر الرقمي كما في حالة الذكاء الاصطناعي تؤدي إلى المساس بالحق في الخصوصية ، مما يثير العديد من التساؤلات حول كيفية حماية هذا الحق في ظل العصر الرقمي.

**أهمية الدراسة**

تعد الخصوصية جوهر الحقوق المدنية التي تنبع منها جميع حقوق الإنسان والحريات الأخرى، منذ القرن العشرين ، ومؤخراً كان للنشر السريع لتقنيات المعلومات والمراقبة باسم الأمن القومي تداعيات خطيرة على الخصوصية الفردية وحقوق الإنسان، وفي هذه الدراسة سيتم تناول الخيوط الرئيسية حول الخصوصية والمفاهيم الحالية للخصوصية الملائمة في سياق تقنيات المراقبة متعددة الأوجه .

وتكمن أهمية الدراسة في تحفيز الوضع القانوني على مجاراة التطور التقني الذي يهدد الحق في الخصيوصية الرقمية من خلال سن السياسات والأنظمة التي تكفل هذا الحق وتعزز من أهميته لدى المجتمعات ، وتحد من سلطة الشركات الخاصة بالتقنيات في حيازة واستخدام البيانات الشخصية للأفراد، بالإضافة إلى نشر التوعية حول حماية البيانات المعلوماتية من قبل الانتهاكات الصادرة للأفراد أو الشركات ومدى أحقية شركات التقنية في استحواذ واستخدام البيانات الشخصية للفرد.

وتتمثل الأهمية العلمية للدراسة في الإثراء القانوني حول الحق في الخصوصية الرقمية، ونشر الوعي حول أهمية هذا الحق ومدى تأثير انتهاكه على كرامة الفرد وكيانه، لذلك فإن هذه الدراسة سوف تتركز حول بيان مفهوم البيانات الشخصية في العصر الرقمي، وصور حمايتها دولياً ومحلياً للوصول إلى معرفة الآليات القانونية لحماية هذه البيانات في كل من التشريع الفلسطيني مقارنة بالتشريع الأردني والمصري، ومن خلال تناول هذه الحماية وفقاً للاتفاقية الأوروبية والقانون الفرنسي، والتي يمكن بموجبها حماية الخصوصية المعلوماتية عند التعامل مع شبكة الإنترنت ، كما وتؤكد هذه الدراسة على الحاجة إلى مزيد من المساءلة ومفاهيم أكثر شمولية للخصوصية والأمن لدعم رفاهية الأفراد والمجتمع والديمقراطية .

أما الأهمية العملية فتتمثل في توجيه المجتمع التقني من خلال الأنظمة القانونية لمراعاة واحترام الحق في الخصوصية المعلوماتية عند تأسيس برامج جديدة ، وإنه ومما لاشك بأن حجم المعلومات الشخصية عن المواطنين والموجودة على شبكة الانترنت مذهل للغاية، نظراً لسهولة الاطلاع عليها من خلال قواعد البيانات الشخصية، ناهيك كذلك عن القيمة المالية الكبيرة لهذه المعلومات المتوافرة في شركات التصنيع التقنية، وتجهيز المعلومات عن هوية العملاء وحول السلع المباعة،

ولهذا فإنه سيتم البحث في طرق معالجة موضوع انتهاك الحق في الخصوصية الرقمية، والموازنة بين هذا الحق وحمايته ، وبين شـــرعية الاطلاع على البيانات الشـــخصـــية من الناحية العملية والقانونية ، وطرح آليات أو إدخال وموائمة نصوص لتكون سارية المفعول في للتشريع الفلسطيني لسد النقص أو تعديل في القانون المطبق على أرض الواقع.

**أهداف الدراسة**

مما لاشك فيه أن هناك معلومات عامة غير متعلقة بالأفراد ، فهذه المعلومات لا يوجد إشكالية من تداولها في معظم الأوقات ، على أن لا يتعارض هذا الاســـتخدام مع الحق في الحصـــول على المعلومات والبيانات، وأية معلومات ضرورية تضمن سلامة الدولة أم منظومة الأمن.

من جهةٍ أخرى ؛ هناك معلومات وبيانات شـــخصـــية يجب أن تخضـــع لقواعد الحماية، والســـماح لصاحبها في حالة جمعها أو معالجتها أو أي طريقة من طرق المعالجة الإلكترونية لها.

من هنا فإن هذه الدراســـة تهدف إلى الوقوف على الجوانب الرئيســـية لبحث موضـــوع الحماية القانونية والجزائية للبيانات الشخصية في العصر الرقمي من منظور القانون الجزائي وذلك لتحقيق الأهداف الآتية:

1- التعرف على مفهوم الخصوصية و البيانات الشخصية الرقمية .

2- وسائل الحماية القانونية لهذه البيانات ، وللحق في الخصوصية في التشريعات المقارنة.

3- مدى حماية البيانات الشخصية في العصر الرقمي في التشريع الفلسطيني والأردني والمصري، وتناول هذه الحماية وفقاً للاتفاقية الأوروبية " بوادبست" والقانون الفرنسي.

**محددات الدراسة**

سيكون نطاق هذه الدراسة منصباً على القوانين السارية المفعول في فلسطين، سيتم تناول موضوع الحماية الجزائية للحق في الخصـوصـية الرقمية ضـمن التشـريع الفلسـطيني من خلال التشـريع الخاص بحماية البيانات الشخصية الخاصة بالمواطنين الفلسطينيين "قرار مجلس الوزراء رقم 3 لسنة 2019" ، وقرار بقانون الجرائم الالكترونية رقم 10 لسنة 2018 وتعديلاته، إضافةً للقانون الأساسي الفلسطيني المعدل رقم 3 لسنة 2003، وذلك بالمقارنةِ مع بعض التشريعات التي عالجت الحماية الجزائية للخصـوصـية الرقمية مثل التشـريع المصـري والتشـريع الأردني، وتناول الحماية الجزائية للخصـوصـية المعلوماتية في التشـريع الفرنسـي ، وكذلك دراسـة المعايير الدولية والمبادئ

الدولية لتطبيق حقوق الإنسان فيما يتعلق بالمراقبة على الاتصالات، وتناول الاتفاقية الأوروبية لمكافحة جرائم الحاسوب.

**منهج الدراسة**

ستتبع الباحثة في هذه الدراسة المنهج التحليلي المقارن ، وذلك من خلال قانون الجرائم الالكترونية الفلسطيني ، لغايات معالجة موضوع الدراسة وتحليل النصوص، مقارنةً بالتشريع المصري الخاص بحماية البيانات الشخصية ، والتشريع الأردني، بالإضافة للقانون الفرنسي الذي توسع في مجال الحماية المعلوماتية، وسيتم تناول الاتفاقية الأوروبية الخاصة بحماية البيانات الشخصية "بودابست"، والمبادئ الدولية لتطبيق حقوق الإنسان فيما يتعلق بالمراقبة على الاتصالات، ، وكذلك التركيز في هذه الدراسة على الكيفية التي تهدف بها الأمم المتحدة والمجتمع الدولي إلى جعل ممارسات المراقبة تتماشى مع قانون حقوق الإنسان وما تعنيه الخصوصية الرقمية في العصر الحديث .

**إشكالية الدراسة**

بالرغم من اختلاف وجهات نظر الفقهاء في تحديد وضبط العناصر المكونة لفكرة الحياة الخاصة، إلا أن المشرع في غالبية الدول قد أحاط تلك الخصوصية في حياة الأفراد بالحماية القانونية مع اختلاف درجات الحماية من تشريع لآخر، لذلك نجد أن كل القوانين العقابية قد جرمت الأفعال والسلوكيات التي تعد انتهاكا للحق في حرمة الحياة الخاصة ، سواء كانت هذه الجرائم تقليدية أو تلك الجرائم التي ارتبطت بنظم المعلومات وتعد أعمالا جرمية مستحدثة يعاقب عليها القانون.

كما أن أغلب التشريعات قد تضمنت هذا الحق وجعلته حقاً دستورياً وجب حمايته من أي انتهاك، وأول تلك التشريعات هو التشريع الإسلامي الذي نهى عن التجسس وأخذ الأخبار وتتبع العورات والأخطاء.

ولذلك فقد حظيت حقوق الإنسان بالاهتمام والالتزام من طرف جميع الدول المكونة للمجتمع الدولي ، وقد تبلور هذا الاهتمام بصدور الإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة ، كما تضاعف حرص المنظمات الدولية للحفاظ على هذه الحقوق بدرجة كبيرة ، من بينها الحق في الحياة الخاصة للأفراد، ومن أبرز هذه الاتفاقيات أيضا الاتفاقية الأوروبية لحقوق الإنسان، والاتفاقية الأمريكية لحقوق الإنسان، والعديد من المؤتمرات الدولية في هذا الإطار، وجميعها تؤكد على حماية حقوق المواطن وحماية الحياة الخاصة للأفراد بصورتها التقليدية، لكنها

حســـب وجهات النظر المختلفة لم تعالج مســـألة حماية الحياة الخاصـــة في ظل نشـــأة وتطور التكنولوجيا المعلوماتية، على الرغم من أنه تشـــكل مخازن وبنوك المعلومات خطراً كبيرا على الحياة الخاصـــة للأفراد، وبخاصـــة في حالة إســـاءة اســـتخدام البيانات المتعلقة بخصـــوصـــياتهم واستغلالها، أو في حالة استخدامها لغايات غير تلك التي جمعت من أجلها.

الأمر الذي يدفع إلى التساؤل عن جدوى النصوص المتعلقة بحماية الحق في الخصوصية وتطبيقها على الخصـوصـية الرقمية، أم أن هذا المفهوم المستحدث يحتاج إلى خلق نصـوص جديدة تتناسـب معه، ولهذا فإن التحدي الأكبر الذي يواجه الحق في الخصـــوصـــية في العصـــر الرقمي يتمثل في غياب واضـــح لقواعد قانونية ملزمة في هذا المجال ، وعليه فإن عدم التقيد بســـبب عدم وجود نصـوص قانونية واضـحة يؤدي في بعض الأحيان في التعسـف والإخلال بالقاعدة القانونية في ظل عدم شـرعية الاجراء وقانونية الوسـيلة ، مما يؤدي إلى الاعتداء وانتهاك الحريات المتعلقة بالأفراد على خصـوصـياتهم سـواء من قبل الأفراد أو من قبل السـلطات العامة، كما أنه يتطلب من المشـرع أيضـاً طرح معالجات تحقق التوازن بين حقوق يعتقد ممارسـوها أن ليس لها نطاقاً، ويعتبرون أن كل شي ملك للجميع من جهة ؟ مع الحرص على ممارسة الحريات والابتكار من جهةٍ أخرى؟

بناءً على ما سـبق فإن حماية الحياة الخاصـة في البيئة الرقمية أصـبح ضـرورة لازمة فرضـتها التطورات التي شـهدها العالم في مجالاته المختلفة ، ولأن التطورات التقنية أصـبحت تشـكل خطراً بالغاً على خصـوصـية البيانات الشـخصـية للأشـخاص ، وحمايتها بالشـكل الذي كفله لهم القانون والدســـتور، أدى ذلك إلى تحديث في مظاهر الحماية القانونية له ومنها الحماية الجزائية لهذا الحق في البيئة الرقمية.

و إن البحث في موضـــوع هذه الدراســـة يثير مجموعة من التســـاؤلات القانونية حول موضـــوع الحماية الجزائية للخصوصية بشكل عام وخصوصية البيانات الرقمية والتي تتم معالجتها إلكترونياً بشـكل خاص، كما أن قواعد البيانات الشـخصـية المعالجة إلكترونياً هي في الوقت الحاضـر غير محمية بشكلٍ كافٍ في معظم الدول، هذا ما قد يشكل خللاً في التشريعات القائمة ويجب العمل على معالجته.

**أسئلة الدراسة**

- هل تمكن المشـــرع الوطني من وضـــع عقوبات رادعة للحد من الجرائم الواقعة على الحياة الخاصة عموماً؟

- ما مدى كفاية ونفاذ التشـــريعات الوطنية وكيفية الموائمة في مجال حماية البيانات الشـــخصـــية المعالجة إلكترونياً أو آلياً وحق الوصول إلى المعلومة وبين حق احترام الخصوصية الفردية؟
- كيف يواجه المشرع جريمة انتهاك الخصوصية عبر الوسائل الإلكترونية الحديثة ؟
- ما هي الضمانات القانونية والإجرائية في ظل الأفعال المرتبطة باستعمال الأجهزة الالكترونية؟

**مبررات الدراسة**

الحق في حماية الحياة الخاصة في البيئة الرقمية أصبح ضرورة لازمة ، نظراً للتطور الذي شهده العالم في المجالات المختلفة ، بسـبب الانتشـار الواسـع لوسـائل التكنولوجيا الخاصـة بالمعلومات والاتصال، إلا أن التطورات التقنية أصبحت تشكل خطرا بالغاً على خصوصية البيانات الشخصية للأفراد ، ويجب حمايتها بالشكل الذي كفله لهم القانون.

**الدراسات السابقة**

**مقدر ، نبيل و بلعسل ، ياسمين، دراسة بعنوان "الحق في الخصوصية الرقمية ، جامعة يحيى فارس ، الجزائر، 2021.[1]**

سلط الضوء في هذه الدراسة على مختلف التغييرات التي حصلت بمفهوم الخصوصية ، وظهور الخصـوصـية الرقمية، وكيف أصـبحت مهددة بالانتهاك في ظل التطور التكنولوجي ، وخلصـت الدراسـة إلى ضـرورة وضـع قوانين خاصـة تجرم الابتزاز والاحتيال والتجسـس الالكتروني ، وركزت على أهمية حماية الخصوصية في البيئة الرقمية نظراً لتدفق المعلومات والبيانات.

**مباركية، مفيدة ، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري(2018).[2]**

تناولت هذه الدراسـة مفهوم الحق في الخصـوصـية الرقمية والحماية الموضـوعية من خلال اسـتعراض الجرائم المتعلقة بانتهاك الخصـوصـية الرقمية ، وتطرقت للحماية الإجرائية للحق في الخصـوصـية الرقمية، وموقف ومدى ملائمة القانون الجنائي الجزائري لحماية هذه الحق ،وقد توصلت الدراسة إلى أنه من الصعب خلق قواعد جناية على المستوى الداخلي لحماية الخصوصية الرقمية ، بل لابد من ابرام اتفاقيات دولية لتنظيم الإطار القانوني لحماية البيانات الشخصية وحماية الخصوصية الرقمية.

[1] نبيل مقدر، وياسمين بلعسل ، دراسة بعنوان "الحق في الخصوصية الرقمية ، جامعة يحيى فارس ، الجزائر،2021.
[2] مفيدة مباركية ، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري ، جامعة الأمير عبد القادرللعلوم الإسلامية، الجزائر ، 2018

**سلمان ، عودة يوسف ، بحث بعنوان الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة في التشريع العراقي " دراسة مقارنة"(2017).[3]**

تناولت هذه الدراسة التعريف بالجرائم الماسة بحرمة الحياة الخاصة والتي تقع عبر وسائل تقنية المعلومات الحديثة، وبيان أهم خصائص وسمات الجرائم الماسة بحرمة الحياة الخاصة ، بالإضافة إلى التعريف بوسائل تقنية المعلومات الحديثة وبيان آثارها على حرمة الحياة الخاصة سواء كانت هذه الآثار ذات أثر إيجابي أو سلبي، كما تناولت هذه الدراسة صور الجرائم الماسة بالحق في حرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة وتناولت الركن المادي والمعنوي لكل من هذه الجرائم.

**فقيه ،جيهان ، بحث بعنوان حماية البيانات الشخصية في الإعلام الرقمي ، دراسة مقارنة ما بين التشريع اللبناني والتشريعات العربية المقارنة(2017).[4]**

سلطت هذه الدراسة الضوء على حقيقة حماية الحق في الخصوصية والبيانات الشخصية عبر مواقع التواصل الاجتماعي ، أظهرت أن الخصوصية والبيانات الشخصية مادة يتم استخدامها إما تجارياً في تنفيذ دعاية تسويقية، أو مراقبتها من قبل جهات حكومية، أو تعرضها للسرقة واستغلالها بغرض الإضرار بأصحابها، وتسليط الضوء في هذه الدراسة على تجارب الدول العربية فيما يتعلق بحماية الخصوصية في العصر الرقمي كما خلصت الدراسة إلى عدم وجود نص دستوري متعلق بحماية الحق في الخصوصية بشكل عام وعدم وجود قانون خاص بحماية البيانات الشخصية في لبنان ، وإدراج التوصيات بهذا الخصوص.

يلاحظ الباحث من خلال الدراسات السابقة أنها تمثل في مجملها شرحاً للحق في الخصوصية وصولا إلى الخصوصية في العصر الرقمي وتطورها من خلال القوانين ومتعلقة بحماية البيانات الشخصية بالإضافة إلى تناول أركان الجريمة المتعلقة بانتهاك الحق في الخصوصية الرقمية ، كما كانت تمثل شرحاً لمواد وبنود المواثيق والمعاهدات الدولية ، أما الدراسة التي ستقدمها الباحثة فهي تختلف عن الدراسات السابقة كونها ستتناول الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني ومن خلال المعايير الدولية، والتنظيم القانوني لها من خلال التشريع الجزائي الفلسطيني ،الذي يطبق قرار بقانون المتعلق بالجرائم الالكترونية الفلسطيني ، مقارنةً بالتشريعات

---

[3] يوسف سلمان عودة ، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة في التشريع العراقي " دراسة مقارنة"، مجلة الحقوق ، الجامعة المستنصرية، بغداد ،2017

[4] جيهان فقيه ، حماية البيانات الشخصية في الإعلام الرقمي ، "دراسة مقارنة"، جامعة العربي بن المهيدي ، الجزائر ، 2017

الجزائية الأخرى التي تناولت ذات الموضـــوع، حيث أنه لم يســـبق الحديث عن الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني.
لذى ارتأت الباحثة تناول هذا الموضوع من خلال هذه الدراسة .

**تقسيم الدراسة**

من أجل تحقيق الهدف من هذه الدراسة والإجابة على التساؤلات المطروحة ستقوم الباحثة بتقسيم الرسالة إلى أربعة فصول كالتالي :

في الفصل الأول ستقوم الباحثة بدراسة **الإطار النظري لفكرة الحق في الخصوصية وماهية الحياة الخاصـــة** ، وذلك من خلال تقسـيم المبحث الأول إلى مطلبين ، يتمثلان في طرح نشـأة الحق في الحياة الخاصـة بدراسـة دور الفقه والقضـاء في إقرار الحق في الخصـوصـية، وفي المطلب الثاني سـيتم تناول مفهوم الخصـوصـية في العصـر الرقمي ، المبحث الثاني سـيتم التطرق إلى مدى خصـوصـية المعلومات ومبررات حماية الحق في الخصـوصـية الرقمية والإطار القانوني لحماية الحق في الخصوصية في التشريعات المقارنة.

في الفصـل الثاني من هذه الدراسـة سـوف تدرس الباحثة **دور البيانات الرقمية في انتهاك الحياة الخاصـــة** وذلك في عدة محاور، تتمثل في المبحث الأول والذي يدور حول أصـر تقنية المعلومات على الحياة الخاصـة وعوامل الاعتداء المعلوماتي على الحق في الحياة الخاصـة ، والمبحث الثاني حول وسائل حماية الخصوصية في العصر الرقمي.

الفصل الثالث سوف يتم البحث وتحليل **النظام القانوني لحماية الحق في الخصوصية الرقمية في المعاهدات الدولية ومن خلال المعايير الدولية بالإضـــافة إلى التشـــريعات المقارنة** ، في المبحث الأول سـوف تدرس الباحثة حماية الحق في الخصـوصـية الرقمية في ظل الاتفاقيات والمعاهدات الدولية، والبحث الثاني حول الحماية الإجرائية للحق في الخصـــوصـــية الرقمية في التشـــريعات المقارنة.

الفصـل الرابع يتناول **الحماية الجزائية للحق في الخصـوصـية الرقمية في التشـريع الفلسـطيني وانسـجامها مع المعايير الدولية** ، المبحث الأول سـتتناول الباحثة واقع الخصـوصـية الرقمية في التشـريعات الفلسـطينية والتحديات التي تواجهها، وفي المبحث الثاني سـيتم تحليل مدى انسـجام التشريعات القلسطينية المتعلقة بالحق بالخصوصية الرقمية مع المعايير والاتفاقيات الدولية.

# الفصل الأول

# نشأة الحق في الخصوصية وتطوره

يقود البحث في الآليات العالمية لحقوق الإنسان وموقفها من الخصوصية الرقمية إلى محاولة ضبط مفهوم هذا الحق، وذلك من خلال تحديد مفهوم الحق في الخصوصية بمفهومها التقليدي العام، ومن ثم التطرق إلى مفهوم وماهية الخصوصية في المجال الرقمي ، باعتبارها جزءاً لايتجزء من الحق في الخصوصية بمفهومه العام.

فالحق في الخصوصية وكما يعرف بالنظام اللاتيني "الحق بالحياة الخاصة" هو حق احترام سرية وخصـــوصـــية الأشـــخاص من أي تدخل مادي أو معنوي ، وهو حق عميق الجذور تاريخياً. والخصـوصـية رسـم للحدود التي تنظم قدرة المجتمع على التدخل في حياة الأشـخاص ، وتشـتمل على أربعة حدود أساسية وهي :[5]

أولاً: خصـوصـية المعلومات "Information privacy " ، والتي تتضـمن القواعد التي تحكم جمع وإدارة البيانات الشـخصـية كمعلومات البطاقات الشـخصـية والمعلومات المالية والسـجلات الطبية والســجلات الحكومية ، وهي المحل التي يتصـــل عادة بمفهوم حماية البيانات data " protection".

ثانياً : خصــوصــية الجســد "bodily privacy " من التدخل الفيزيائي ، والتي تتعلق بالحماية الجسـدية للأفراد ضـد أي إجراءات تمس النواحي المادية لأجسـادهم ، كفحص الجينات، وفحص المخدرات .

ثالثا: خصـوصـية الحيز المكاني أو الخصـوصـية الإقليمية ؛ والتي تنظم القواعد المتعلقة بدخول الفرد إلى المنازل أو الأماكن العامة و تتضـــمن قواعد التفتيش والرقابة الالكترونية والتأكد من بطاقات الهوية.

رابعا: خصـوصـية الاتصـالات " Telecommunication privacy" وهي تغطي سـرية وخصوصية المراسلات الهاتفية ، والبريد الالكتروني والاتصالات الخلوية وغيرها من وسائل الاتصال.[6]

---

[5] محمود عبد الرحمن ، نطاق الحق في الحياة الخاصة ، دار النهضة العربية ، مصر 1994 ، ص 123.

[6] يونس ، عرب ، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الالكتروني بواسطة الهاتف الخلوي ،اتحاد المصارف العربية ، الأردن ، 2001.

ومع تطور تكنولوجيا المعلومات وماتبع ذلك من تطورات طالت البيانات الضـــخمة ، ومجالات استغلالها، أصبحت مبادئ البيانات الشخصية تتعارض مع مبادئ الخصوصية .

وفي هذا الفصـل سـوف يتم التطرق للأسـاس القانوني في الحق في الخصـوصـية ونشـأة الحق في الحياة الخاصة، ومدى خصوصية المعلومات الخاصة، والحق في الوصول إليها.

## المبحث الأول: نشأة الحق في الحياة الخاصة

يعد موضوع الحق في الخصوصية أحد أهم المواضيع في الوقت الحاضر؛ نظراً لارتباطه الوثيق بكرامة الإنسان والتي تعتبر أمراً جوهرياً لهُ علاقة مباشرة بحياة الإنسان التي منحها له الله تعالى ، ومن ثم تبنت هذا الحق الأحكام الوضعية، حيث أنه لا يجوز الإنتقاص من كرامة الإنسان، وأي انتقاص منها يؤدي بشكل فعال ومباشر إلى الإعتداء على خصوصية الأفراد.

هذا ولقد أثَر التقدم التكنولوجي المتسارع في السنوات الأخيرة على حياة الأفراد، وحرياتهم الخاصة، مما أدى إلى تغير الحياة الاجتماعية، جراء التطفل على الحياة الخاصة للأفراد وانتهاكها. ونظراً لأهمية الحق في الحياة الخاصة على مستوى الأفراد والجماعات ، ودوره في استقرار المجتمعات ، فقد اهتمت لهذا الموضوع النصوص الدينية منذ الأزل ، وتكفلت الأحكام الوضعية بسن القوانين والتشريعات لحماية الحق في الحياة الخاصة.

### المطلب الأول: دور التشريعات والقضاء والفقه في إقرار الحق في الخصوصية

ستطرق الباحثة في هذا المطلب إلى التعريفات المتعلقة بالحق في الخصوصية ، وإلى دور التشريعات الوضعية والفقهية في إقرار الحق في الخصوصية ، وذلك من خلال تناول دور القضاء والتشريعات الوضعية في إقرار الحق في الخصوصية في الفرع الأول من هذا المطلب، و تناول دور الفقه في إقرار الحق في الخصوصية في الفرع الثاني من هذا المطلب.

#### الفرع الأول : دور الأحكام الوضعية في إقرار الحق في الخصوصية

على صعيد الأحكام الوضعية في حماية الحق في الخصوصية ، فقد أقرت العديد من الدول التشريعات لحماية وإقرار الحق قي الخصوصية، ومن هذه الدول ( الجزائر ، مصر ، الأردن وفلسطين ، والمشرع الفرنسي ).

فيما يتعلق بالمشرع الفلسطيني ، فقد صدر قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية ، وقد جاء في المادة 22 منه :" 1- يحظر التدخل التعسفي أو الغير قانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته 2- كل من أنشأ موقعا أو تطبيقا أو حسابا الكترونيا أو نشر معلومات على الشبكة الالكترونية أو احدى وسائل تكنولوجيا المعلومات بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية، سواء كانت مباشرة أو مسجلة، تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة،يعاقب بالحبس مدة

لا تقل عن سنة وبغرامة لا تقل عن ألف دينار أردني ولا تزيد عن ثلاثة آلاف دينار أردني، أو ما يعادلها بالعملة المتداولة".[7]

كما ويجرم القانون الأساسي الفلسطيني الذي يعد بمثابة الإطار الدستوري للنظام القانوني الفلسطيني الاعتداء على حرمة الحياة الخاصة، وحسبما جاء في القانون في المادة 32 من القانون الأساسي الفلسطيني لسنة 2003 :" حظر الاعتداء على الحريات الشخصية وحرمة الحياة الخاصة، كل اعتداء على أي من الحريات الشخصية أو حرمة الحياة الخاصة للإنسان وغيرها من الحقوق والحريات العامة التي يكفلها القانون الأساسي جريمة لا تسقط الدعوى الجزائية ولا المدنية الناشئة عنها بالتقادم ."[8]

- المشرع المصري ؛ فلم ينص صراحة في تشريعاته على حق الخصوصية ، ولكن قد خصص الدستور المصري الحالي الصادر عام 2014 م مادة مستقلة للحق في الحياة الخاصة، بالإضافة إلى ما تضمنته الدساتير من نصوص أخرى تكفل جوانب معينة من الحق في الخصوصية ، كحرمة المسكن الخاص ، وسرية المراسلات وغيرها.[9]

فقد نصت المادة 57 من الدستور المصري على " للحياة الخاصة حرمة، وهي مصونة لاتمس ، وللمراسلات البريدية والبرقية، والالكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال، حرمة وسريتها مكفولة ، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب".[10]

كما نصت المادة 58 أيضا على " للمنازل حرمة، وفيما عدا حالات أو الاستغاثة لايجوز دخولها ولا تفتيشها، ولا مراقبتها أو التنصت عليها إلا بأمر قضائي مسبب، ويحدد المكان والتوقيت والغرض منه وذلك كله في الأحوال المبينة في القانون ".[11]

- أما بالنسبة للمشرع الأردني فقد صدر في العام 2015 قانون الجرائم الالكترونية ، حيث يتضمن هذا القانون سبعة عشر مادة موزعة بين ما هو إجرائي وما هو موضوعي ، واشتمل على مواد لحماية الحياة الخاصة منها :

أ- المادة 4 :" والتي تعاقب كل من مكّن الآخرين من الاطلاع على بيانات ومعلومات".

---

[7] قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية ، تشريع فلسطيني ، م 22
[8] القانون الأساسي الفلسطيني المعدل لسنة 2002، م 32
[9] مقالة بعنوان الحق في الخصوصية والأمان الشخصي ، مركز هردو للدعم الرقمي ، القاهرة، 2015، ص 11-23
[10] المادة 57 من الدستور المصري لسنة 2014
[11] المادة 58 من الدستور المصري لسنة 2012

ب- المادة 5 : " يعاقب من قام قصـداً بالتقاط أو اعتراض أو بالتنصـت أو أعاق أو صـوَر أو شطب محتويات على ما هو مرسل عن طريق الشبكة المعلوماتية ".[12]

- المشرع الفرنسي قد ذكر الحرية الشخصية في ديباجة الدستور الصادر في أكتوبر سنة 1958، وكذلك الدستور الصادر في سنة 1946، وقد استخلص المجلس الدستوري الفرنسي مبدأ صيانة الحرية الشخصية من سياق نص المادة 66 من الدستور ، والتي تنص على أنه : "لايجوز القبض على أحد أو حبسه إلا وفقاً للقانون ."

كما أن القضاء الفرنسي يعتبر أول من اعترف بحماية الحياة الخاصة أو الحرية الشخصية ، ولم يجعلها مقتصرة على الحماية المادية فقط بل جعلها تمتد لحماية العناصر المعنوية من مختلف صور المساس بالحياة الخاصة .[13]

- في الدول التي ليس لها دستور مكتوب كالمملكة المتحدة ، فإن العرف الدستوري بالإضافة إلى وثائق حقوق الإنسان تقضي باحترام الحرية الشخصية مثل العهد العظيم ووثيقة الحقوق، ويعد العهد العظيم الصادر عام 1215 من أقدم الوثائق التي نصت على حماية الحرية الشخصية في بريطانيا، فقد نصت المادة 39 منه على أنه : "لايجوز القبض على شخص أو حرمانه من أملاكه واعتباره خارجاً على القانون أو نفيه أو التعرض له بأي طريق إلا بناء على حكم صحيح وفقاً لقانون البلاد."[14]

وبهذا و على الرغم من وجود حماية قانونية لحق الحياة الخاصة وهي جزء أصيل للحق في الخصوصية ، إلا أن إعطاء تعريف جامع ومانع لمدلول الخصوصية من الناحية القانونية أمر صعب ، ويعود ذلك إلى:

- التوسع والامتداد الذي تمتاز به الخصوصية.
- لانها موضوع مرن ، ويختلف من مجتمع لآخر، ومتغير بالنظر إلى العامل الزمني.
- الخصوصية لا تختلف من مجتمع لآخر فقط ، وإنما تختلف من فردٍ لآخر، ومن شخص عادي إلى شخص آخر مشهور.

إضافة إلى ذلك فإن الحق في الخصوصية يعدُ مرتبط أشد الارتباط بحق حرية الصحافة والإعلام، والذي يعد تقييداً لها ، ومن هنا أكدت لجنة الخبراء المنبثقة عن المجلس الأوروبي لحقوق الإنسان

---

[12] قانون الجرائم الالكترونية الأردني لسنة 2015 المواد 3 و4.

[13] يوسف الشيخ يوسف، حماية الحياة الخاصة في القانون الجنائي المقارن، رسالة دكتوراه،، جامعة القاهرة،دار الثقافة للنشروالتوزيع ، الأردن، 1996، ص 200.

[14] صالح بن عبد الله ، الراجحي ، حقوق الإنسان وحرياته في الشريعة الإسلامية والقانون الوضعي ، مكتبة العبيكان ، المملكة العربية السعودية ، 2004 ، ص 88.

، أنه لا يوجد تعريف عام متفق عليه على الصـــعيد التشـــريعي أو القضـــائي أو الفقهي أو المجال الدولي أو الوطني .[15]

من خلال ما ســـبق ترى الباحثة أن الحق في الحياة الخاصـــة وقدســـيتها وحمايتها من الاختراق والانتهاك من أهم الحقوق التابعة للإنسـان، والموازية لكل الحقوق الأخرى الشـخصـية، حيث تمتد جذور هذا الحق إلى حضـارات قديمة ومواثيق وتشـريعات عالمية، وقد تابع رحلته ليتصـدر قائمة الحقوق المصانة في عالم المعلوماتية، وهو من الحقوق الشخصية التي تبقى لصيقة بصاحبها حتى وفاته ، حيث أن الحياة الخاصة للإنسان مرتبطة بكرامته ، وشرفه ، وله كامل الحق في المحافظة على هذه الجوانب الجوهرية في حياته، لذا عملت كل الدول على وضع قواعد أو قوانين تهدف إلى إيجاد قواعد تحمي الحياة الخاصة وتمنع المساس بها.

**الفرع الثاني : دور الفقه في إقرار الحق في الخصوصية**

إن الخصوصية عبارة عن منظومة متكاملة ومتناسقة من الخصائص، لها سمات وخصائص مادية ومعنوية، وهي عبارة عن أســـلوب حياة، ومجموعة من الأخلاقيات التي تتمثل في النظرة للعالم ، ورؤية الذات والآخر، كما أن الحق في الحياة الخاصة هو من الحقوق اللصيقة بالإنسان والموازية لكل الحقوق الأخرى الشخصية.

لقد مرت الخصوصية بثلاثة مراحل تاريخية، تطورت من خلالها فكرة الخصوصية إلى أن وصل مفهومها إلى العصر الرقمي، وهذه المراحل هي :

المرحلة الأولى : الخصوصية المادية ؛ وهي الاعتراف بالخصوصية ، كحق حماية الأفراد من أي اعتداء مادي على حياتهم وممتلكاتهم.

المرحلة الثانية: الخصوصية المعنوية وهي عبارة عن حماية القيم والعناصر المعنوية للفرد.

المرحلة الثالثة: الخصوصية كحق عام يمتد نطاقه لحماية الأشخاص من كافة أوجه الإعتداءات ، أو أي تدخل في حياتهم أياً كان مظهرها، أو طبيعتها، وفي نطاق الأخير ولد مفهوم جديد للخصوصية ارتبط بأثر التقنيات الحديثة على الحياة الخاصة، والتي تتمثل بخصوصية المعلومات، أو حق الأفراد في حماية البيانات الشخصية ، والسيطرة عليها في ظل تحديات العصر الرقمي.[16]

---

[15] ياسين قوتال ، حق الخصوصية الالكترونية بين التقييد والإطلاق، جامعة عباس الغرور ، خنشلة، الجزائر ، ص57

[16] بارق منتظرعبد الوهاب اللامي ، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني – دراسة مقارنة - ، رسالة ماجستير ، جامعة الشرق الأوسط ،عمان ، الأردن ، 2017 ، ص 12

أما فيما يتعلق بمفهوم الخصـــوصـــية فإنها من الناحية اللغوية يقصـــد بها؛ حالة الخصـــوص، والخصوص نقيض العموم، ويقال : خصَهُ بالشئ يخصه خصاً وخصوصاً.[17]

أما من الناحية الاصطلاحية ؛ فإن وضع تعريف دقيق وواضح للحق في الخصوصية يعوَل عليه ، يعدُ أمراً صعباً، ولذلك فإن الخصوصية من الناحية القانونية لم يرد لها تعريفاً خاصاً ، أو تحديداً لمعناها أو بيانها، لا في معظم الدساتير ولا في التشريعات، ورغم أن معظم الدساتير لم تستخدم لفظ الخصوصية ، يحكم أن الفرد في حياته الخاصة يكون في خصوصية ، بالمقابل قد يفهم من الخصـــوصـــية بأنها الحياة الخاصـــة المرتبطة بمكان معين، وقد اتجه الفقهاء إلى تعريف الحياة الخاصة ، وتحديد الانتهاكات الواقعة على الحق في الخصوصية .

فقد عرَف القاضـي الأمريكي (كولي ) الحياة الخاصـة بأنها " الحق في أن يترك المرء وشـأنه" ، والفقه الأمريكي عموماً عرَف الحياة الخاصـــة عن طريق ذكر مجموعة من صـــور الانتهاكات الرئيسية التي تقع على الحق في الخصوصية ، وذلك حسبما ورد في التطبيقات القضائية في الولايات المتحدة الامريكية ، وقد ذهب الفقهاء إلى أن الانتهاكات التي تقع على هذا الحق هي كما يلي :[18]

- انتهاك أو اقتحام عزلة الفرد أو خلوته ، أو التدخل في حياته الخاصـــة ، كالاعتداء على حرمة مسكنه، أو التنصت على محادثات هاتفية أو تصويره أو التأمين على حياته بغير رضا .
- الإفشاء العلني للوقائع التي تمس الشخص العادي ، كالمعلومات الصحية.
- تشويه سمعة شخص في نظر الجمهور .
- الاستيلاء على بعض عناصر الشخصية كالاسم والصور ، لتحقيق مغنم خاص ، مثل استغلال اسم الشخص أو صورته في الدعاية لسلعة.

مما سبق يتضح أنها تفصيلاً للانتهاكات التي تقع على الحق في الخصوصية وليست تعريفا أو توضيحاً للمقصود بالحق في الخصوصية.

ذكر الفقيه ( نيزا Niza ) أن الحق في الخصـــوصـــية هو " حق الفرد في حياة منعزلة مجهولة، فالشـــخص من حقه أن يعيش بعيداً عن أنظار الناس ، وعن القيود الاجتماعية ، بمعنى أنه من حق الشخص ألا يكون اجتماعياً".[19]

---

[17] ابن منظور، لسان العرب، دار الأميرية- ط2، ج8، 30 ميلادي، ص 290.

[18] حسام الدين كامل الأهواني ، الحق في احترام الحياة الخاصة ، دراسة مقارنة ، دار النهضة العربية، 1978،القاهرة ، ص58

[19] سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري، رسالة ماجستير، جامعة وهران، الجزائر،2013، ص 1

وذكر الفقيه روجر كولار(Roger Colar) ، أن الحياة الخاصة بدأت تتضح تأسيساً على الحق في الملكية الذي يعني : " عدم نشر أية أخبار أو صور عن شخص دون إذنه أو موافقته."[20]

في الشريعة الإسلامية على الرغم من عدم ذكر لفظ الحق في الخصوصية من قبل فقهاء الشريعة قديماً، إلا أن هذا لا يعني أنه لم يعترف بهذا النوع من الحق ، بل على خلاف ذلك فإن الدين الإسلامي قد اعترف منذ البداية بالحق في الخصوصية، ويظهر ذلك جلياً من خلال تكريم الإنسان وصيانة حرماته، ويؤكد الرسول صلى الله عليه وسلم على أهمية المحافظة على حرمة خصوصيات الفرد ؛ عن عبد الله بن عمر قال : " رأيت رسول الله صلى الله عليه وسلم يطوف بالكعبة ويقول { ما أطيبك ومأطيب ريحك، وما أعظمك وأعظم حرمتك، والذي نفس محمد بيده لحرمة المؤمن أعظم عند الله حرمة منك، ماله ودمه وأن نظن به إلا خيرا }.[21]

وإن الباحث في أحكام الشريعة الأسلامية، يجد أنها أوردت ضوابط عامة ، يؤدي تطبيقها على وجهٍ صحيح إلى المحافظة على حرمة الحياة الخاصة ، ولعل من أبرز تطبيقات الحق في الحياة الخاصة في الدين الإسلامي هو حق الفرد في حرمة مسكنه، والعيش فيه آمناً بعيداً عن تدخل الآخرين، وهذه الحرمة تقررت بقوله تعالى : { يا أيها اللذين آمنوا لا تدخلوا بيوتا غير بيوتكم حتى تستأذنوا وتسلموا على أهلها، ذلك خيرُ لكم لعلكم تذَكرون }. صدق الله العظيم [22]

كما نجد أن التشريع الإسلامي أقرَ حق الإنسان في الحرية الشخصية ، وقد اشترط أن تكون ممارسة هذا الحق ملتزمة بحدود الشريعة الإسلامية ، وألَا يترتب على هذا الحق حدوث ضرر للشخص ذاته أو للآخرين .[23]

وفي الكتب السماوية أيضاً ثمة العديد من الإشارات للخصوصية تنطوي على اعتراف بحماية الانسان من أن يكون مراقباً ، فقد ورد بالتوراة كأقدم كتاب سماوي ، وثمة حماية للخصوصية في الشرائع اليونانية والصينية القديمة ، فهو حق قدم قدم البشرية.

---

[20] سليمان أحمد فضل ، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة،ط1، 2007، ص215.

[21] ابن ماجه،سنن ابن ماجه، باب حرمة ذم المؤمن وماله، الحديث رقم 3932، تحقيق : محمد فؤاد عبد الباقي، دار الفكر، بيروت، ج2 ، ص 1297.

[22] سورة النور ، الآيه 27

[23] جمال عبد الناصر عجالي ، الحماية الجنائية من أشكال المساس بحرمة الحياة الخاصة عبر المكالمات والصور ، دراسة مقارنة، جامعة محمد خيضر، الجزائر ،2014 ، ص 22

**المطلب الثاني : الخصوصية في العصر الرقمي**

إن مفهوم الحق في الخصوصية الرقمية هو امتداد لمفهوم الحق في الحياة الخاصة ، إلا أنه يختلف بكونه يتصل بالمعلومات الالكترونية الخاصة بالأفراد ويتعلق بمدى حرية الشخص و في الحق بأن يتحكم بالمعلومات التي تخصـــه من المبادئ ، ولبيان أثر وســائل التقنيات المعلوماتية الحديثة على الحق في الخصوصية سيتم تقسيم هذا المطلب إلى فرعين، نبحث في الفرع الأول نشأة الخصوصية المعلوماتية ونطاقها عبر الانترنت ، ويتناول الفرع الثاني الآثار الإيجابية والآثار السـلبية لوسـائل التقنيات الحديثة على الحق في الخصوصية.

**الفرع الأول : نشأة الخصوصية المعلوماتية ونطاقها عبر الانترنت**

يعزى الفضل في مفهوم خصوصية المعلومات إلى مؤلفين أميركيين في هذا المجال ، وهما الأول : كتاب الخصوصية والحرية ، لمؤلفه ويستن عام 1967، والثاني كتاب الاعتداءعلى الخصوصية لمؤلفه ميلر، وكلاهما قدما مفهوماً وتعريفا لخصوصية المعلومات ، فقد عرف ويستن الخصوصية المعلوماتية بأنها : " حق الأفراد في تحديد متى وكيف وإلى تصل عنهم المعلومة للآخرين The claim of individual to determine for themselves when, how and to what extent information about them is communicated of others "

في حين عرَف ميلر الحق في خصوصية المعلومات على أنها : " قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم "

"The individuals ability to control the circulation of information relating to him "

وتعرف الخصـوصـية الرقمية بأنها وصـف لحماية لبيانات الشـخصـية للفرد ، والتي يتم نشـرها وتداولها من خلال وسـائط رقمية، وتتمثل البيانات الشـخصـية في البريد الالكتروني ، والحسـابات البنكية والصـور الشـخصـية، ومعلومات عن العمل والمسـكن التي نسـتخدمها من خلال الانترنت أثناءاسـتخدام الحاسـب الآلي أو الهاتف المحمول ، أو أي وسـيلة من وسـائل الاتصـال بشـبكة الانترنت.[24]

كما تعرف الخصـوصـية الرقمية بأنها "ذلك الحق الذي يحمي الحياة الخاصـة للفرد من خلال إحاطته بسياج من السرية، ومعاقبة كل من يحاول الاعتداء عليه ، بدون علم وإرادة صاحبها."[25]

[24] عاطف كريم ،الخصوصية الرقمية بين الانتهاك والغياب التشريعي،مركز دعم لتقنية المعلومات ،القاهرة، 2013، ص2

[25] نصر الدين ،ماروك ، الحق في الخصوصية ، مجلة النائب ، الجزائر ، 2003 ، ص 17

كما يمكن تعريفها بأنها : "وصف لحماية البيانات الشخصية للأفراد التي يتم نشرها وتداولها من خلال الوسائط الرقمية".[26]

ويقترن مفهوم الحق في الخصوصية [27] الرقمية بشكل مباشر بالمعلوماتية ومختلف استخداماتها، وتحتل جانباً مهماً من الحياة الخاصة منذ ستينيات القرن الماضي.

ومما لا شك فيه أن البيانات الشخصية هي المحل الذي ينشأ حوله الحق في الخصوصية الرقمية باعتبارها مصدراً للمعلومات الخاصة، لذلك فإن نطاق هذا الحق واسع ومتعدد باعتبار أن البيانات الشخصية تتواجد في الفضاء الرقمي ، ولذلك يمكن القول أن الحق في الخصوصية الرقمية يتعلق على وجه الخصوص بالبيانات الشخصية المخزنة في قواعد البيانات والأنظمة المعلوماتية للمؤسسات والإدارات كالملفات الطبية والمحاكم والمعلومات المتعلقة بالموظفين ، كما يتعلق الحق في الخصوصية الرقمية بالاتصالات والمراسلات عبر الانترنت.

في نهاية الستينات والسبعينات كان قد انطلقت دراسات قانونية اهتمت بالخصوصية وبحقوق الإنسان ، تحت ضوء التطورات التقنية، وقد تناولت مفهوم خصوصية المعلومات الالكترونية بشكلٍ مستقل عن باقي مفاهيم الخصوصية، ولقد ظهرت مع التكنولوجيا ما يسمى بنوك المعلومات والتي يقصد بها ؛ تكوين قاعدة بيانات تفيد موضوعاً معيناً، وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الالكترونية ، لإخراجها بصورة معلومات تفيد مستخدمين مختلفين في أغراض متعددة ، فيما تحتوي عليه من معلومات حول الأفراد وما يخزن عنه من البيانات التي قد تشكل عنصر تضييق وتقييد لمشاركته في شؤون الحياة العامة ، وقد يشكل أمر التخزين خطراً بشكل أو بآخر على حياة الفرد الخاصة ويهددها ، ويصبح الفرد أسيراً للمعلومات التي جمعتها الحاسبات الآلية ، ورصدت كل تحرك من تحركاته .[28]

ومما لا شك فيه أن مواقع التواصل الاجتماعي هي عبارة عن مواقع تربط الأفراد في كل مكان على كوكب الأرض ، حيث تمتد هذه المواقع من دولة إلى أخرى ومن مدينة إلى أخرى، وإن تزايد أعداد الأشخاص المستخدمين لهذه المواقع بصورةٍ غير طبيعية يترتب عليه انتهاك الحياة الخاصة

---

[26] نصر الدين ماروك ، المرجع السابق ، ص 18.

[27] الحق في الخصوصية ذكر في المرة الأولى في مقال نشر عام 1890 لبراندیس وورن Brandis warn، في مجلة هارفرد الحقوقية في الولايات المتحدة الأمريكية، وهو مفهوم مرتبط بكيان الإنسان أو حيزه الخاص الذي يسعى من خلاله إلى حماية مشاعره وأفكاره وأسراره الخاصة تجسيداً لكينونته الفردية .

[28] محمد رشيد أبو حجيلة،الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات، دراسة مقارنة، رسالة ماجستير، كلية الحقوق ،جامعة آل البيت، عمان ، الأردن، 2007 ، ص 4.

للمستخدمين عبر شبكة الانترنت ، فالأمر لايقتصر فقط على موقع محدد ، بل هناك الكثير من المواقع الالكترونية التي اقتحمت دول العالم أجمع [29].

وعلى الرغم من الدور الذي تشغله هذه الشبكات الالكترونية في حياتنا الاجتماعية، بالنظر إلى أنها أصبحت سمة مميزة في العصر الرقمي[30]، حيث أنه من خلالها بالإمكان التفاعل بين المستخدمين في حياتهم اليومية، على الرغم من أنها تثير بعض المخاوف حول أمن وخصوصية البيانات الشخصية التي يدلي بها المستخدمون.

إذ أن المعلوماتية بأدواتها المتسارعة وقدرتها على استيعاب قدر أكبر من المعلومات والبيانات الاسمية ، واسترجاعها وتصنيفها وتحليلها ومعالجتها ، والقيام بعملية تداولها دون وجود عوائق يشكل تهديدا حقيقياً لحقوق الأفراد في احترام حياتهم الخاصة .

وذلك يكشف بوضوح إلى أي مدى يمكن أن يكون تهديد الخصوصية ، والحقيقة أن استخدام التقنيات العالية في جمع ومعالجة البيانات الشخصية من قبل الدول وقطاعاتها الخاصة، قد عمَق التناقضات الحادة التي برزت فيما تعلق بين حق الأفراد في الحياة الخاصة ، وموجبات الاطلاع على بيانات الأفراد ، وتتمثل هذه التناقضات يما يلي وذلك من خلال أربعة معالم رئيسية [31] :

أولاً : التناقض بين الحياة الخاصة وفي حق الدولة في الاطلاع على شؤون الأفراد، والذي عمَقه تدخل الدول في شؤون الأفراد، وليس المراد الاطلاع على معلومات معينة عن الأفراد لتنظيم الحياة الاجتماعية بشكل أفضل ، كالاحتفاظ بسجلات المواطنين ، الولادة ، الزواج، الوفيات ، وغيرها ، بل استخدام الدول للمعلومات الخاصة للفرد لأغراض تتناقض مع صونها واحترمها.

ثانياً: التناقض بين حق الفرد في الاحتفاظ بسريته ، ومصلحته في كشف حياته الخاصة ليتمتع ويحقق ثمار هذا الكشف ، ورغم أن هذا التناقض غير متحقق للوهلة الأولى باعتبار أن الاحتفاظ بالسرية حق ، والكشف الطوعي عن هذه السرية حق أيضاً، إلا أن احتمال استغلال المعلومات المعطاة طوعاً لأغراض غير التي أعطيت من أجلها يمثل انتهاكا لخصوصية الفرد .

ثالثاً: التناقض بين الحياة الخاصة، والحق في جمع المعلومات لغايات البحث العلمي .

رابعاً: التناقض بين الحق في الحياة الخاصة ، وبين حرية الصحافة وتبادل المعلومات وهي ما تعرف بالحربات الإعلامية.[32]

---

[29] د.طارق جمعة السيد راشد، مدى حجية رسائل التواصل الاجتماعي في الإثبات، دراسة تحليلية مقارنة، مجلة العلوم القانونية، جامعة عين شمس ، القاهرة، عدد 2، 2016، ص 45

[30] د.أحمد عصام، تأثير مواقع التواصل الاجتماعي على خصوصية الفرد الجزائري، رسالة ماجستير، كلية العلوم الإنسانية ، جامعة المسيلة، الجزائر ، 2013، ص 17

[31] يونس عرب ، مرجع سابق ، 2001.

[32] نصر الدين ماروك، الحق في الخصوصية ، مرجع سابق ، ص،17

وقد أعطى الفضاء الالكتروني رجال السلطة صلاحيات كبيرة في مجال مراقبة الأفراد على شبكة الانترنت، بواسطة برامج خاصة تمكنهم من رصد تحركات الأفراد واختراق البريد الالكتروني دون إذن قضائي في بعض البلدان، وإن أهم مجالات التعرض للخصوصية هي ؛ خصوصية البيانات ومنها خصوصية الاتصالات والبريد الالكتروني، والهواتف المحمولة المتصلة بشبكة الانترنت، والخصوصية الصحية، والخصوصية المالية، وهناك مجالات أخرى متعددة لا يمكن حصرها في التعرض للخصوصية على شبكة الانترنت.

وعليه يظهر الواقع أن انتهاك الخصوصية أمر مستمر ، حتى في الدول الديمقراطية التي تعمل وفق تشريعات حماية الحياة الخاصة، نظراً لغياب أدوات تطبيق القانون ، وإن كانت الجهود التنظيمية ، والتشريعية قد سعت إلى إقامة التوازن بين هذه الحقوق المتعارضة ، إلا أن استخدام التقنيات الحديثة لجمع ومعالجة البيانات الشخصية ، يخلق واقعاً صعبا يهدد هذا التوازن .

في الدول العربية التشريعات غير قادرة على مواجهة الانتهاكات الحاصلة على الحق في الخصوصية، وهناك ضرورة للعمل على نشر الوعي الثقافي بالحق في الخصوصية الرقمية.

فلقد ارتبط مفهوم الجريمة المعلوماتية بما تشتمل عليه وسائل الاتصال والإعلام من بيانات ومعلومات ، يتم جمعها وتداولها وتخزينها ومعالجتها آلياً ورقمياً أو الكترونياً، وهذا الأمر سهل وسرع ووسع الوصول إليها واختراقها، وقد تكون هذه البيانات مرتبطة بدول وكيانات أو أشخاص معينين، وهو ما دفع بالدول والمجتمعات لإعادة النظر بمنظوماتها القانونية والتشريعية لغايات تجريم مثل هذه الأفعال.

ويواجه مستخدموا الانترنت الفلسطينيون تحديات على مستويات عدة، فيما يتعلق بحماية البيانات الخاصة بهم، فعلاوة على الانتهاكات من قبل شركات عالمية التي يتعرض لها المستخدمون، يواجه الفلسطينيون الانتهاكات الإسرائيلية وانتهاكات محلية أيضا، حيث يتحكم الاحتلال بالبنى التحتية لتكنولوجيا المعلومات والاتصالات الفلسطينية، إلى جانب فرض رقابة الكترونية تجمع بيانات وتنتهك خصوصية كل فلسطيني بحجة دواعي أمنية ،إذ ترى المنظمات الحقوقية بأن تبني قانوناً لحماية البيانات الشخصية في فلسطين ، لن يوفر سوى مستوى محدود من من الحماية ، وذلك نظرً لخضوع البنية التحتية الخاصة بتكنولوجيا المعلومات والاتصالات للسيطرة الكاملة من قبل سلطات الاحتلال الإسرائيلي ، رغم توقيع اتفاقية أوسلو عام 1993 ،إذ تتحكم السلطات الإسرائيلية في الموجات الكهرومغناطيسية للفضاء الرقمي ، وتتحكم في عمليات استيراد وتركيب أي معدات لشركات الاتصالات الفلسطينية، وشركات مزودي الخدمة، كما يتم استخدام تقنيات

تجسس ومراقبة واستغلال للبيانات الشخصية ، دون أي مساءلة قانونية [33]، أما على الصعيد المحلي فإن غياب سلطة تشريعية قادرة على سن قوانين وتشريعات مواكبة للتطورات في عالم التكنولوجيا يفتح الباب على مصراعيه لانتهاك خصوصية الأفراد وحماية البيانات الشخصية في القطاع الحكومي والخاص، وحتى هذه اللحظة لا يتوافر قانون خصوصية وحماية بيانات شخصية ورقمية واضح وشامل بل نصوص مواد فضفاضة عند خضوعها للفحص الصارم المتعلق بالضمانات العادلة .

وبالإشارة إلى هذا الموضوع ، فإنه يعاني الفلسطينيون من مجموعة من التحديات الرقمية المرتبطة بالوصول إلى منصات التواصل الاجتماعي والرقابة عليها ، كما يعاني المواطن الفلسطيني من تقييد الوصول إلى نشر المحتوى المتعلق بالقضية الفلسطينية ، ومعاناة في صياغة المحتوى على شبكات التواصل ، مما يؤدي إلى صعوبة وصول الحقائق المتعلقة بالوضع الفلسطيني إلى العالم ، فالرقابة الرقمية المفروضة من قبل الشركات العالمية على المواطن الفلسطيني غير متوازنة ، مما يظهر حجم التحديات التي يواجهها المواطنون الفلسطينيون فيما يتعلق بالرقابة على المحتوى الخاص بهم عبر الفضاء الرقمي.[34]

وبهذا يتحدد نطاق الحق في الخصوصية الرقمية بين حدين متناقضين يتمثل أولا في حق الأفراد في الحياة الخاصة ، وثانيا في موجبات الاطلاع على شؤون الأفراد وما تفرضه الضرورة على الدول والحكومات في توفير حد أدنى من الأمان الرقمي بذات الوقت كبح للجريمة المرتكبة عبر الفضاء الرقمي، وهذا النطاق يتحدد كما يلي :

- إيجاد تناسق بين الحق في الخصوصية وحق الدولة في الإطلاع على هذه الخصوصية في إطار تنظيم الحياة على نحوٍ أفضل، وهذا لايتعارض في مفهومه مع التعرض للحياة الخاصة للأفراد بأي حال إلا في حال استخدام البيانات الشخصية لأغراض تتنافى مع صونها واحترامها.
- إيجاد تناسق بين حق الفرد في عدم الكشف عن أي بيانات تتعلق بخصوصيته مع القدرة في الكشف عن هذه الخصوصية لمصالح عملية، إذ يتبين عدم وجود تعارض بين الحق في السرية والكشف الإرادي عن هذه الخصوصية ، إلا أن هذه الفكرة تخص مسألة تفادي

[33] ،مروة فطافطة ،ديما سمارو،حماية البيانات في الشرق الأوسط وشمال افريقيا، منظمة اكس ناو ،2022 .
[34] الانتهاكات الرقمية للفلسطينيين ، دراسة مقدمة من قبل مركز صدى الإعلامي ، رام الله ، فلسطين ، 2024.

أي احتمال لاستغلال تلك المعلومات المصرح بها إرادياً ليتم استغلالها في أغراض تهدد حرية الشخص وتشكل انتهاك لخصوصيته.[35]

من خلال ما سبق تستخلص الباحثة أن الحياة الخاصة أصبحت لها منحنى مختلف، وهي شكل مستحدث للخصوصية لها علاقة مباشرة بالبيانات الرقمية ، ولها معنى آخر في ظل التطور التكنولوجي، ولا تشتمل على الخصوصية بالمعنى الشامل، وانما تشتمل على الخصوصية المعنوية المرتبطة بوسائل التواصل في الفضاء الالكتروني .

**الفرع الثاني : الآثار الإيجابية والسلبية لوسائل التقنيات المعلوماتية الحديثة على الحق في الخصوصية**

لقد ترتب على تطور وسائل الاتصال الحديثة كشبكة الانترنت والهواتف المحمولة ، والأقمار الصناعية وغيرها من الوسائل ، تقديم خدمات كبيرة للعالم أجمع ،لاغنى لأي مجتمع عنها، وبالتالي تبرز آثارها الإيجابية على الحق في حرمة الحياة الخاصة، إذ أن من حق المستخدم الحفاظ على سرية معلوماته وبياناته واتصالاته التي يجريها، ومما لاشك فيه أن لاستخدام التقنيات المعلوماتية الحديثة آثاراً إيجابية ، لا يستطيع أحد إنكارها سواء على صعيد الأفراد أو على صعيد الدول وتنظيمها لشؤون الأفراد.

فاتجهت الدول إلى إنشاء قواعد بيانات لتنظيم عملها، واتسع استخدام الوسائل التقنية الحديثة في جمع وتخزين ومعالجة البيانات الشخصية لأغراض متعددة، إذ أن المعلومات المتعلقة بجميع جوانب الحياة الخاصة للأفراد يمكن جمعها وتخزينها لفترة غير محدودة، ويمكن الرجوع إليها بمنتهى السرعة والسهولة .[36]

وبالرغم من أهمية التقنيات الحديثة وما سبق بيان الآثار الإيجابية لهذه التقنيات ، إلا أن هنالك مخاطر عدة تواجه الحق في الخصوصية بحيث إمكانية انتهاك هذا الحق عبر الفضاء الرقمي ، وذلك أن سهولة معالجة وتخزين وازدياد تدفق المعلومات التي تتم عبر التقنيات الحديثة، تضعف قدرة الفرد على التحكم في تدفق المعلومات الخاصة به.

وقد أصبح طريق الوصول إلى المعلومات الشخصية بالأفراد وبصورة غير مشروعة أكثر من ذي قبل ، وازدادت فرص إساءة استخدامها.

---

35 منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الأقتصادية، 2013،ص 19.

36 عبد الرؤوف المهدي، الجوانب الإجرائية لحماية الحق في الحياة الخاصة، بحث مقدم إلى مؤتمر الحق في الحياة الخاصة، كلية الحقوق ، جامعة الإسكندرية ، 1987، ص3

كما ازدادت عملية مراقبة الأفراد وملاحقتهم، وعمليات التعدي على خصـــوصـــياتهم ، من خلال الوصـول إلى البيانات المخزنة وسـجلاتها ، بالإضـافة إلى ذلك ؛ فإن تلك الوسـائل سـاعدت على عولمة المعلومات والاتصالات عبر الحدود دون أية اعتبارات جغرافية أو سياسية متعلقة بالسيادة للدول، بحيث تعطى المعلومات لجهات داخلية وخارجية بل ولجهات مجهولة، وهو ما يؤدي إلى إساءة استخدام البيانات الخاصة خاصةً في البلدان التي لا توفر حماية قانونية للبيانات الشخصية ، مما يؤي إلى انتشـــار الجرائم الماســـة بحرمة الحياة الخاصـــة عبر الفضـــاء الرقمي كالتجســـس الالكتروني ، إذ تسـتخدم في البيئة الرقمية العديد من الوسـائل التقنية لتتبع المعلومات الشـخصـية للمشـتركين ، ولا صـحة للاعتقاد السـائد أنه بإمكان أي فرد الدخول إلى المواقع الالكترونية باسـم مســـتعار أو عبر عنوان زائف للبريد الإلكتروني، إذ يمكن لمزودي الخدمة معرفة أي شـــخص يسـتخدم الشـبكة الالكترونية ويسـتطيع الدخول إلى كافة المنتديات والمواقع ومعرفة المشـتركين بدقة.[37]

ترى الباحثة أنه بالنظر إلى انتشـار اسـتخدام الوسـائل التقنية الحديثة وبالرغم من الآثار الإيجابية لانتشارها ، إلا أنه قد ازدادت جرائم الاعتداء على البيانات الشخصية واختراق الخصوصية عبر الفضـاء الرقمي ، هذا الأمر يبرز معه أهمية التوفيق والتوازن بين أهمية وفائدة اسـتخدام الفضـاء الرقمي ، وبين تفادي ما يمكن أن يصـيب الأفراد من أضـرار أو تعدي على حرمة الحياة الخاصـة نتيجةً لاستخدام هذه الوسائل .

[37] إبراهيم شمس الدين ، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات ، دار النهضة العربية ، القاهرة، 2005 ،ص 45

## المبحث الثاني: أهمية ومبررات حماية الحق في الخصوصية الرقمية

قد تؤدي مشـــاركة المعلومات الشـــخصـــية إلى تحقيق فوائد ، وغالباً ما يكون من الضـــروري مشـــاركتها لغايات التفاعل مع الأشـــخاص الآخرين ، ولكن هذا الأمر يكاد لا يخلو من المخاطر، حيث أن البيانات الشخصية يمكن أن تكشف عن المعتقدات والتفاصيل المتعلقة بالأفراد.

وحيث أنه من السـهل اسـتخدام هذه البيانات بكل سـهولة للإيذاء ، مما يشـكل خطراً على الأفراد والمجتمعات ، خاصـــة وأن مسـتقبل الخصـــوصـــية على الشـبكة العالمية غامض جداً ، وهنالك صـعوبات تواجه رواد التقنية والمشـرعون لتأمين سـبل الحماية للمسـتخدمين ، وما هي مبررات حماية الحق في الخصـوصـية الرقمية وأهميته ، وكيف نظمت التشـريعات المحلية والمقارنة الحق في الخصـوصـية والوصـول إلى المعلومة ، هذا ما سـيتم تناوله من خلال هذا المبحث من خلال المطلب الأول والذي يتناول مبررات حماية الخصـــوصـــية الرقمية وحق الأفراد في الوصـــول للمعلومة وخصائص الخصوصية في العصر الرقمي ، ويبحث المطلب الثاني في الاطار القانوني لحق الخصوصية في العصر الرقمي في التشريع الفلسطيني والتشريعات المقارنة.

### المطلب الأول: مبررات حماية الحق في الخصوصية الرقمية

استخدام التقنيات الحديثة والتكنولوجيا في ميدان جمع ومعالجة البيانات الشخصية المتعلقة بالحياة الخاصـة للأفراد له آثاراً إيجابية كما سـبق توضـيحها ، لا يسـتطيع أحد إنكارها خاصـةً في مجال تنظيم الدولة لشـؤون الأفراد في جميع المجالات الأجتماعية والاقتصـادية والعلمية وغيرها، وهذا ما يسـمى ببنوك المعلومات أو قواعد البيانات، [38] فتكون مقصـورة على بيانات ومعلومات تتصـل بقطاع معين، كبنوك المعلومات الصحية أو القانونية مثلاً، أو شاملة لقطاعات مختلفة ، وقد تكون مهيئة للاســتخدام على المســتوى العام أو على المســتوى الخاص ، وقد تكون للاســتخدام على المسـتوى الإقليمي أو الدولي ، وعليه اتجهت دول العالم بمختلف هيئاتها ومؤسـسـاتها إلى إنشـاء قواعد البيانات لتنظيم عملها ، وصـــاحب هذا التوجه ظهور الشـــعور بمخاطر تقنية المعلومات وتهديدها للخصوصية.[39]

في هذا المطلب سـتتناول الباحثة في الفرع الأول مبررات حماية الحق في الخصـوصـية ، وأهمية ومدى حرية الأفرد في الحصول على المعلومات في العصر الرقمي من خلال الفرع الثاني .

---

[38] "بنوك المعلومات :هي مجموعة المعلومات التي تتم معالجتها وذلك من أجل بثها على شبكة الانترنت"

[39] د.ياسين قوتال ، المرجع السابق ص 61.

**الفرع الأول: أهمية ومدى حرية الأفرد في الحصول على المعلومات في العصر الرقمي**

إن مفهوم الخصوصية واحترام الغير الخاص لكل فرد مرتبط بشكل وثيق بنظومة حقوق الإنسان والحريات، مما يستدعي منع أي فرصة لانتهاك الخصوصية من قبل أي جهة، خاصة في ظل الثورة التكنولوجية والعصر الرقمي ، حيث زادت الحاجة لتطوير أدوات حماية البيانات الضخمة المتوفرة عبر الفضاء الالكتروني على الرغم من كونها خاصة وشخصية للأفراد، والتي يتم في الكثير من الأحيان استخدامها دون الحصول على إذن مسبق من أصحابها مما يعد انتهاكاً واضحاً لحق الخصوصية لأصحابها ، مما حرك الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد من شأن مراعاتها الحق في الحياة الخاصة ، وإيجاد التوازن بين حاجات المجتمع لجمع وتخزين المعلومات ومعالجة البيانات الشخصية ، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها [40].

هذا وتكشف البينات الشخصية والرقمية ، المتوفرة على شبكة الانترنت أو لدى الشركات والمؤسسات والحكومات، الكثير عن الأفراد وأفكارهم ونمط حياتهم وتحركاته، وأصبح من السهل استغلال هذه البيانات، لإيذائهم، والإيقاع بهم والتأثير عليهم وعلى خياراتهم، فعلى سبيل المثال، استغلت بعض الحكومات البيانات الشخصية الرقمية لصحفيين وناشطين مناهضين لها، لملاحقتهم ، كما ولا يقتصر استغلال البيانات على الحكومات والمؤسسات، بل حتى الأفراد يمكنهم استغلال بيانات شخصية لأفراد آخرين، لابتزازهم وإلحاق الضرر بهم، لذلك أصبح من الضروري الحرص على حماية البيانات الشخصية والرقمية لكل فرد، وتوفير الحق لهم في اختيار الجهة التي يرغبون بمشاركة معلوماتهم معها ، ومن لديه حق الوصول إليها، إلى جانب المدة الزمنية التي يمكن الاحتفاظ بها في قواعد البيانات ، فضلاً عن قدرة الفرد على تعديل هذه البيانات متى شاء.[41] وفي ظل استخدام الحاسب الآلي والوسائل الالكترونية وبنوك المعلومات في تخزين وتحليل ومعالجة واسترجاع الكميات الهائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر الحكومية أو من قبل مؤسسات القطاع الخاص والربط بينها ، ونقل المعلومات عبر الانترنت من مكان لآخر، تزداد فرص استخدام البيانات والمعلومات الشخصية على نحو غير مأذون به، بل يفتح الباب على مصراعيه لإساءة استخدام تلك المعلومات أو توجيهها توجيها منحرفاً أو خاطئاً أو مراقبة الأفراد وتعرية خصوصياتهم أمام الغير[42].

---

40 نهلة عبد القادر المومني ،الجرائم المعلوماتية ، دار الثقافة ، عمان ، الأردن ، ط1، 2008 ، ص 165 + 166.

41 آمنة الصيادي،البيانات الشخصية:ما مدى أهمية حمايتها وهل من تشريع؟، منظمة اكسس ناو،2021

42 انطونيوس أيوب يوليوس، الحماية القانونية للحياة الشخصية في مجال المعلوماتية ، منشورات الحلبي الحقوقية،بيروت، 2009، ط1 ، ص 43

وعليه يعد احترام وتطبيق حقوق الإنسان في أي بلد معياراً أساسيا لتعميم واقع الديمقراطية وأداء منظومة العدالة، كما يعتبر الحق في الخصوصية من الحقوق الأساسية للإنسان، التي نصت عليها القوانين المحلية والمواثيق والمعاهدات الدولية.[43]

و الحق في الخصوصية هو من الحقوق المنصوص عليها بشكل صريح في الاتفاقيات والمواثيق الدولية، حيث نصت المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه " لا يجوز تعريض أحد للتدخل التعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملة تمس شرفه أو سمعه ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات."[44]

وعلى الصعيد الوطني فقد عالج القانون الأساسي الفلسطيني رقم 3 لسنة 2003 موضوع الحق في الخصوصية وحمايتها بشكل واضح وصريح في مادتين في باب الحقوق والحريات ، حيث نصت المادة 10 على " 1- حقوق الأنسان وحرياته الأساسية ملزمة وواجبة الاحترام 2- تعمل السلطة الوطنية الوطنية الفلسطينية دون إبطاء على الانضمام إلى الإعلانات والمواثيق الإقليمية والدولية التي تحمي حقوق الإنسان".[45]

وكذلك في نص المادة 32 أيضا من نفس القانون [46]، والتي حفظت الحق في الحرية الشخصية وحرمة الحياة الخاصة للإنسان، وغيرها من الحقوق والحريات التي يكفلها القانون الأساسي الفلسطيني.

كما يشكل قرار بقانون لمجلس الوزراء رقم 3 لسنة 2019 حول حماية البيانات الشخصية الخاصة بالمواطنين ، فهو يخاطب على وجه الخصوص الشركات والمؤسسات ، حيث يظهر من خلال هذا القرار مخاطبة لشركات مزودي الخدمة حول حظر الحصول على البيانات الخاصة بالمواطنين دون الحصول على إذن مسبق منهم تحت طائلة المسؤولية.

وعليه يمكن استنتاج من خلال ما سبق ومن خلال القراءة المعمقة لمفهوم الخصوصية سواء بالمفهوم العام ، أو بمختلف جوانبها بالنظر إلى التطور التكنولوجي الحاصل ؛ أن الخصوصية هي متغير تابع لبيئة تمثل متغيراً ثابتا، وأن التحولات في هذه البيئة تؤدي تاريخيا وتراكمياً إلى تغيرات في مكونات هذه الخصوصية ، بمعنى أن ثبات مكونات الخصوصية هو متغير نسبي ،

---

[43] أبو عرقوب، عمر ، دراسة استكشافية، واقع الخصوصية وحماية البيانات الرقمية في فلسطين، مركز حملة –المركز العربي لتطوير الإعلام الاجتماعي ، آب 2021.

[44] الإعلان العالمي لحقوق الإنسان www.ohchr.org

[45] انظرالقانون الأساسي الفلسطيني المعدل رقم 3 لسنة 2003

[46] انظر القانون الأساسي الفلسطيني رقم 3 لسنة 2003

وهي ليست كتلة صماء بل هي تجسيداً لحوار مجتمع معين وتفاعله مع ماضيه وحاضره ومستقبله ، وانعكاس لتفاعل هذا المجتمع مع واقعه وعالمه ، والخصوصية مكون أساسي من مكونات المجتمع ، أي لا يمكن تصور وجود مجتمع لايمتلك خصوصيته ، وتمثل ما هو عام ومشترك ومتوافق عليه إلى حد كبير، وربما أصبح مكونا أساسياً من مكونات الهوية الشخصية. [47]

**الفرع الثاني: مبررات حماية الحق في الخصوصية الرقمية**

في العالم الرقمي حالياً ، يعتقد أن المخاوف بشأن الخصوصية جديدة ، لكن من الواضح أنها ليست كذلك ، على الرغم من أن " الخصوصية" في حد ذاتها لم تكتسب معناها الحديث إلا في بدايات القرن التاسع عشر ، لذلك فإن الفكرة قديمة قدم التاريخ، بمعنى أن فكرة أن بعض الأمور يجب أن تكون خاصة ومحمية ليست جديدة ، وكذلك ضرورة الموازنة بين الخصوصية مقابل بقية المخاوف ، لكن حين يتعلق الأمر بالخصوصية فإن سرعة التغيرات التكنولوجية تطغى على المعايير الثقافية والقوانين، إذ أحدثت التكنولوجيا تحولاً في معنى " المعلومات العامة" ، ففي عصر البيانات الرقمية هذه المعلومات لها اعتبار وجودة خاصة بها .[48]

ومع تزايد التقنيات الحديثة زادت المخاطر على الحق في الحياة الخاصة ، وأصبح الفرد مقيداً في تعاملاته من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة التقنيات الحديثة كتقنيات المراقبة والتجسس والمساس بالمعلومات الخاصة للأفراد، وهذه جميعها تشكل تهديداً على الحياة الخاصة والحريات المتعلقة بالأفراد ، لاسيما إذا استغلت لغايات خارجة عن إرادة صاحبها ودون علمها، وبناءً على ذلك نجد أن مبررات حماية الحق في الخصوصية الرقمية على النحو الآتي :

- اتساع شبكة الانترنت: حيث أن أهم التقنيات التي تتحكم في جميع التعاملات الالكترونية تعتمد بشكل مباشر على شبكة الانترنت وهي ليست بمنأى عن ولوج أي متطفل أو معتدي يستغل وسائل الاتصالات، إذ أن تدفق المعلومات والاتصالات عبر الحدود دون أي اعتبارات سياسية أو جغرافية، بحيث يتم تبادل المعلومات بين الأفراد والمعطيات الخاصة بهم لجهات مختلفة، وفي قنوات داخلية أو خارجية، وهو ما يثير مخاطرإساءة استخدام هذه البيانات خصوصاً في الدول التي لا تتوفر فيها الحماية القانونية للبيانات الشخصية.[49]

[47] السيد ياسين، المعلوماتية وحضارة العولمة ، دار النهضة ، مصر ، ط2، 2008 ، ص 10.
[48] ايثيوبيس تافارا، مقالة بعنوان أهمية حماية الخصوصية في عصر البيانات الرقمي، مدونات البنك الدولي ، 2020.
[49] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية ، مصر ، 2000، ص 4

- الطبيعة الخاصة للتعاملات الالكترونية: فهذه الطبيعة الافتراضية تفتقد إلى المادية، فتجعل من الشخص وهو بصدد استخدام شبكة الانترنت يتوقع قدراً من الخفية أكثرمن العالم الواقعي، بينما الواقع يظهر عكس ذلك ، إذ أن التعاملات الالكترونية تترك آثاراً ودلالات على شكل سجلات رقمية حول الموقع الذي تم زيارته ، والأمور التي تم البحث عنها ، والمواد التي قام بتنزيلها ، والوسائل التي أرسلها أو البضائع التي اشتراها من خلال المواقع الالكترونية، مما يجعله عرضة للخطر والاستغلال .
- فقدان آليات السيطرة في قنوات التعامل الالكتروني : إن حق الخصوصية في العالم الرقمي يكتسب ذو وضع خاص ، وإن تكريس قانون خاص يقر استراتيجية ملائمة لحماية الأفراد بعيداً عن العالم الرقمي يعد سهلاً، بوضع الرقابة من قبل الدولة على الاعتداءات، لكن فيما يتعلق بحماية الخصوصية الرقمية فلا يعد ذلك بالأمر السهل ، لانها مرتبطة بعالم افتراضي ممتد يرتبط بشبكة الانترنت عبر الحدود ، وهنا يحتدم الصراع على السيطرة على الانترنت من خلال الصعوبة في التحكم في نطاق المواقع الالكترونية وعناوينها ، مما يؤدي إلى توسع دائرة اختراق حق الأفراد ويصعب من الحماية ضد الانتهاكات لخصوصياتهم .[50]

**المطلب الثاني : الحماية الجزائية للحق في الخصوصية الرقمية في ظل تنامي تطبيقات الذكاء الاصطناعي**

نظراً لما يشهده العالم اليوم من تقدم وثورة تكنولوجية متسارعة ، فقد بات الذكاء الاصطناعي يطغى على التوجهات العالمية لتحسين مؤشرات التنمية في جميع المجالات، ومما لا شك فيه بأن هذا التوجه نحو الذكاء الاصطناعي لا يخلو من المخاطر والسلبيات ، إذ يشكل تهديداً حقيقياً للحق في الخصوصية الرقمية لأنه يسهل الاطِّلاع على البيانات ، ويكشف أدق تفاصيلها ، وفي هذا المطلب سيتم تناول مدلول الذكاء الاصطناعي ، وما هي الفجوة بين استخدام الذكاء الاصطناعي وحماية الحق في الخصوصية الرقمية ، وحول تأثير تقنيات الذكاء الاصطناعي على الحق في الخصوصية الرقمية.

[50] أحمد حسام طه تمام ، الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية ، مصر ، 2000، ص 359.

**الفرع الأول : مدلول الذكاء الاصطناعي**

الذكاء الأصـــطناعي هو فرع من فروع علم الحاســبات ، وهو العلم الذي يجعل الآلات تفكر مثل البشـــر، كما يجعل الحاســـوب يمثل محاكاة للقدرات الذهنية والعقلية وأنماط عملها ، ومن أهم خصـائصـها القدرة على التعلم والاسـتنتاج ورد الفعل على أوضـاع لم تبرمج عليها الآلة ، أي أنها برامج وأنظمة تحاكي الذكاء البشـري لأداء المهام ، ويمكنها أن تحسـن من نفسـها اسـتناداً إلى المعلومات التي تجمعها .[51]

و لقد جاء الذكاء الاصـــطناعي كنتيجة للثورة الصـــناعية الرابعة " Fourth Industrial Revolution"، حيث يعود اسـتعماله لأول مرة أكاديمياً إلى سـنة 1950، من خلال " آلان تورينغ" ، الذي قدم له من خلال اختبار Turin ، وهو اختبار حمل اسمه ، وقد تمحور حول تقييم الذكاء لجهاز الكمبيوتر ، إذ يحســب قدرته على محاكاة العقل البشـــري ، كما قد تم اســـتعمال المصطلح لأول مرة في مؤتمر الدول للذكاء الاصطناعي ، بحضور خبراء البرمجيات .

وبعد دخول عصـــر البيانات الضـــخمة ، أصـــبحت البيئة الرقمية أكثر كفاءة ، ليدخل الذكاء الاصـــطناعي بأبعاده الملموســـة وغير الملموســـة في مختلف مجالات الحياة حتى وصـــل إلى منظومتي القانون والقضاء.[52]

كما وجد تعريف أخر للذكاء الاصـطناعي على أنه : "القدرة على التصـرف كما لو كان الإنسـان هو الذي يتصـــرف من خلال محاولة خداع المســـتجوب وإظهار كما لو أن إنســـاناً هو الذي يقوم بالإجابة على الأسئلة المطروحة من قبل المستجوب ."[53]

بعض التشـــريعات وضـــعت تعريفاً للذكاء الاصـــطناعي في إطار معالجة البيانات الشـــخصـــية، فالمشـرع المصـري عرف المعالجة الالكتروني بطريق الذكاء الاصـطناعي بأنها : "المعالجة : أي عملية الكترونية أو تقنية لكتابة البيانات الشخصية ، أو تجميعها، أو تسجيلها ،أو حفظها أو تخزينها أو دمجها أوعرضـها أو أرسالها ، أو استقبالها ، أو تداولها أو نشرها، أو محوها ، أو تغييرها ، أو تعديلها ،أو استرجاعها أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الالكترونية أو التقنية سواء تم ذلك جزئيا أو كلياً."[54]

---

[51] هناء ، رزق محمد،مفهوم الذكاء الاصطناعي ، مجلة دراسات في التعليم الجامعي ، العدد 52، مصر ،2021، ص574.

[52] محمد ، بومديان ، الذكاء الاصطناعي تحد جديد للقانون ، مجلة مسارات للأبحاث والدراسات القانونية، تونس ، ص 227 -228، المغرب ،2021.

[53] عائشة ، مصطفى بن قارة ،الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية ، مجلة البحوث القانونية والسياسية ، العدد السادس، 2006، ص 275.

[54] انظر المادة 1 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 ، الجريدة الرسمية ، 2020.

ومما سبق يمكن القول ويمكن القول بأنه لغاية وقتنا الحالي لا يوجد تعريف موحد للذكاء الاصطناعي ، مع اتضاح صورته والاستخدام المطَرد لتطبيقاته، لكن يمكن الاستنتاج بالعموم ، بأن الذكاء الاصطناعي هو عبارة عن العلم الذي يهدف إلى تصميم أنظمة ذكية ، من شأنها أن تجعل الحاسبات الآلية تحاكي التفكير البشري ، وتتعامل بذات القدرات البشرية من خلال تغذيته بالبيانات الشخصية والمعلومات ، أو من خلال التعلم الذاتي.

**الفرع الثاني: تأثير تقنيات الذكاء الاصطناعي على الحق في الخصوصية الرقمية**

إن استخدام برامج الذكاء الإصطناعي في مختلف مجالات الحياة يثير العديد من الصعوبات لاسيما فيما يتعلق بالمسؤولية الجزائية عن أعمال هذه البرامج و مدى ملائمة التشريعات الحالية و قدرتها على إستيعاب الخصائص الفريدة لهذه التقنيات ،لاسيما في ظل تسارع وتيرة التطور التكنولوجي فلقد أعطت البرامج المتطورة لبعض الآلات التي تعمل بالذكاء الإصطناعي قدرات هائلة تصل خطورتها حد بناء خبرة ذاتية تمكنها من إتخاذ القرارات بصورة مستقلة ، لذا من المتصور أن تخرج هذه الكيانات عن السيطرة البشرية و ترتكب الجرائم بإرادة منفردة بعيداً عن الأوامر البرمجية المعطاه لها ، إذ يوجد العديد من تطبيقات الذكاء الاصطناعي الماسة بخصوصية الأفراد ، وهي عبارة عن أجهزة تجسس ورصد تقوم بالاطلاع على البيانات المتعلقة بالأفراد ، كذلك يستخدم الذكاء الاصطناعي خاصية التعرف على الوجه ، ويعمل هذا النظام على تحليل ميزات الوجه ، ومقارنتها مع الوجوه المعروفة الموجودة في قاعدة البيانات داخل الأنظمة الأمنية ، كما أنه يوجد تطبيقات تقوم بتدقيق البيانات والفيديوها التي يتم التقاطها ، وبذلك فإنه ينتج عنه سلبيات متعددة من استخدامه دون ضوابط قانونية وهي انتهاك للحياة الخاصة.[55]

هذا وتقدم اللائحة الأوروبية العامة لحماية البيانات والتي دخلت حيز النفاذ في عام 2018 معايير موحدة لحماية البيانات ، والفكرة الأساسية منها هي منح الأشخاص سيطرة فعالة على بياناتهم الشخصية ، وامتثالا لهذه القواعد فإنه يتعين على الشركات والمؤسسات اتباع المبادئ الرئيسية المتعلقة بحماية البيانات الشخصية وذلك منصوص عليه في المادة رقم 5 من اللائحة العامة، وهي الشفافية ، وتقييد الأهداف ، وتقليل البيانات ، والدقة ، وتقييد التخزين ، والسرية ، وذلك يعني بأن الحق في الخصوصية وحمايته من الانتهاكات وحماية البيانات الشخصية يقتضي عدم السماح

[55] يحيى ، إبراهيم دهشان ، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي ، مجلة الشريعة والقانون، جامعة الإمارات ، 2020 ، ص 115.

باستخدام البيانات الشخصية على نحو يهدر تلك الحقوق ، وخاصة عند معالجتها في ظل تقنيات الذكاء الاصطناعي.[56]

وبإمعان النظر إلى انتهاك الحق في الخصوصية الرقمية نجد أن المستخدم في حال أساء التصرف بارتكاب أحد جرائم انتهاك الخصوصية الرقمية باستخدام تقنيات الذكاء الاصطناعي ، فإن الإشكالية تثور حول تصرف تقنيات الذكاء الاصطناعي بانتهاك الخصوصية بمعزل عن مستخدم هذه التقنية فهل يجوز ملاحقة تلك التقنية ؟ والجواب يكون بالنفي لكونه ليس إنسان ولا يتمتع بالأهلية وفقاً لمبدأ الشرعية الجنائية ، واستناداً لذلك تتجه الآراء إلى المناداة بضرورة منح التقنيات الذكية الشخصية القانونية الالكترونية على غرار الشركات الاعتبارية ، مع فرض عقوبات خاصة بهذه التقنيات كون أن لها الإدراك الاصطناعي.[57]

وكل ذلك يدعو إلى الاستنتاج بأن الذكاء الاصطناعي نجح في التأثير السلبي على العديد من جوانب الحياة في ظل غياب الضوابط للتحكم في تطبيقات الذكاء الاصطناعي، وغياب تشريعات تنظم التعامل مع هذه التطبيقات، مما يتطلب ضرورة صياغة إطار أخلاقي وقانوني للتعامل مع هذه التقنيات الحديثة، لتحقيق التوازن وتفادي سلبياته، بالإضافة إلى أن الحق في الخصوصية سرية البيانات محل اهتمام التشريعات والمواثيق ،مما يقتضي عدم السماح باستخدام تلك البيانات على نحو يهدر تلك الحقوق، لا سيما عند معالجتها من خلال تطبيقات الذكاء الاصطناعي.

---

[56] د.محمد فتحي ،إبراهيم ، التنظيم التشريعي لتطبيقات الذكاء الاصطناعي ، مجلة البحوث القانونية والاقتصادية ، القاهرة ، العدد 81، 2022، ص 1028.

[57] د. أحمد ،براك ، إشكالية المسؤولية الجزائية لتقنيات الذكاء الاصطناعي ، مركز البحوث القانونية، العراق، 2023، ص 155

## الفصل الثاني

## دور البيانات الرقمية في انتهاك الحياة الخاصة

من الملاحظ أنه وفي الآونة الأخيرة ومع تزايد التطور التكنولوجي الهائل وانتشـــار التكنولوجيا بشكل واسع في المجتمعات ، والاعتماد عليها في تسهيل أمور وشؤون المجتمع ، حيث أنها حلّت تدريجيا محل الأيدي العاملة من البشـر، والكثير من المؤسـسـات والشـركات باتت تعتمد على هذه الحاســبات لما لها من قدرات هائلة تجعلها قادرة هلى عملية جمع وتخزين ومعالجة كم هائل من البيانات الخاصـــة بالأفراد، مما يجعل لها أثراً من حيث طبيعتها والعديد من العوامل على حياة الأفراد الخاصة.

استناداً لما ذكر أعلاه سوف يتم تقسيم هذا الفصل إلى مبحثين ، المبحث الأول سوف يخصص لبحث أثر أنظمة المعلومات على الحياة الخاصة ، وفي المبحث الثاني سيتم الحديث فيه عن صور الاعتداء المعلوماتي على الخصوصية ووسائل حماية الحياة الخاصة في العصر الرقمي.

### المبحث الأول : أثر أنظمة المعلومات على الحياة الخاصـــة و عوامل الاعتداء المعلوماتي على الحق في الخصوصية

الخصوصية كما ذكر سابقاً، هي حق الفرد في الحفاظ على معلوماته الشخصية، وحياته الخاصة ، بشـكل اختياري وحر، ومفهوم الحياة الخاصـة في الأنظمة المعلوماتية قد توسـع وتطور ليشـمل معاني جديدة لم تكن ذات اعتبار في فترات زمنية ســابقة، وقد ســرع العصــر الرقمي من تآكل الخصـوصـية المعلوماتية للمسـتخدمين على شـبكة الانترنت ، وذلك بسـبب الكم المعلوماتي الهائل المتوفر في الفضـــاء الرقمي ، حيث ظهرت أنواع جديدة من المعلومات على الشـبكة الالكترونية تخص الأفراد وتكون مهددة بالانتهاك.

ونظراً إلى أن الانترنت قد ســهل وظيفة جمع البيانات الشــخصــية ومعالجتها ونقلها، فالتصــفح والتجول عبر الانترنت قد يترك لدى المواقع التي تم زيارتها كمية واســعة من المعلومات ، حيث يترك المســتخدم آثاراً ودلالات كثيرة تتصــل به ، ويشــكل ســجلات رقمية عن الموقع الذي قام بزيارته والأمور التي بحث عنها، والمواد التي قام بتنزيلها ، والبضـــائع التي قام بشـــرائها عبر الانترنت، مما يجعل هذه البيانات والمعلومات الخاصة عرضة للاختراق أو التزوير أو التشهير .

سـوف يتم تقسـيم هذا المبحث إلى مطلبين ؛ الأول سـوف تتناول الباحثة فيه خطورة أنظمة المعلومات على الحياة الخاصـة وعوامل الاعتداء المعلوماتي على الخصـوصـية، وفي المطلب الثاني سـتتطرق الباحثة فيه إلى بيان وتوضـيح طبيعة المعلومات المشـمولة بالحماية الجزائية للخصوصية الرقمية.[58]

**المطلب الأول: الاعتداء على الخصـوصـية الرقمية وطبيعة المعلومات المشـمولة بالحماية الجزائية للخصوصية الرقمية**

لقد شـهد العالم تطوراً كبيراً في مجالات الاتصـال و والتواصـل بين الناس ، خاصـة في مجال تكنولوجيا المعلومات المتمثل بشـبكة الانترنت وما يشـمل الهواتف والحواسـيب، مما كان لها أكبر الأثر على الحياة بشـكل عام ، وعلى حياة الأفراد بشـكلٍ خاص، وعليه فإن هذا الأمر كان له أثر إيجابي على الحياة البشـرية يتمثل في سـرعة التواصـل بين أفراد المجتمع، وسـرعة نقل الأخبار والمعلومات ، مما أدى إلى تقريب المسـافات وسـبل التعارف بين أفراد المجتمع ، وجعله أكثر سـهولة، إلا أنه في ذات الوقت كان له أثر سـلبي على المجتمع ، ويتمثل هذا الأثر باعتبار أن الاعتداء على الخصـوصـية الرقمية يشـكل جريمة الالكترونية ، ومن خلال هذا المطلب سـيتم توضيح صور الاعتداء المعلوماتي على الخصوصية من خلال الفرع الأول ، وتناول كيفية اعتبار الاعتداء على الخصوصية المعلوماتية يشكل جريمة الكترونية بشئ من التفصيل .

**الفرع الأول : صور الاعتداء المعلوماتي على الخصوصية**

في العصـر الرقمي الحديث، أصـبحت الاعتداءات المعلوماتية على الخصـوصـية أكثر تكراراً مع تزايد كمية البيانات الشـخصـية المخزنة على شـبكة الانترنت والتي تأتي من مصـادر متعددة ، كوسائل التواصل الاجتماعي، والأجهزة المحمولة ، ومعاملات التجارة الالكترونية، وهذا الاعتداء يكون من خلال جمع المعلومات الشـخصـية وتحليلها وإسـاءة اسـتخدامها بأي طريقة أو صـورة، بالإضـافة إلى تخزين البيانات والملفات والمعلومات على أجهزة الكمبيوترمن قبل الحكومات والمؤسسات والشركات، إذ ازداد الاعتماد على الانترنت لجمع البيانات وتخزينها لتسهيل الوصول إليها وتبادلها بمختلف الوسائل، هذا ويتم استخدام شبكات الانترنت وبنوك المعلومات بشكل واسع كوسيلة لانتهاك الخصوصية، لأنها تسمح بجمع وتخزين وتحليل المعلومات الشخصية التي تستخدم

[58] امحمد أمين الشوابكة، جرائم الحاسوب والانترنت الجريمة المعلوماتية، الطبعة الأولى، 2007 ، دار الثقافة ، عمان ، ص 95

لأغراض متعددة، مثل انتحال الهوية والتلاعب السياسي والتشهير بالآخرين، كما تأخذ انتهاكات الخصوصية من قبل السلطات أو الأفراد عدة أشكال ، كتخزين أو استرداد المعلومات أو تغيير أو تعديل محتواها ، أو استخدامها دون إذن صاحبها أو مالكها ، كاختراق الحاسبات أو اختراق البريد الإلكتروني إذ أن هذه الجريمة تقوم على أساس الاعتداء على الخصوصية وسرية البيانات لأغراض غير مشروعة وتلحق بالأفراد عدة خسائر على المستوى المادي والمعنوي ، سرقة أرقام بطاقات الائتمان ، انتحال صفة الغير ، وإفشاء المعلومات المالية مثل البطاقة المصرفية وغيرها.[59]

كما تتعدد صور الاعتداء المعلوماتي على الخصوصية الرقمية من خلال الاعتداء على سرية المعلومات الشخصية ، ويتمثل ذلك الأمربالمعالجة غير المشروعة للبيانات ، أو تعرض المحادثات الشخصية للأفراد للتجسس عبر شبكة الانترنت بالإضافة إلى اختراق الأنظمة الخاصة بالأفراد ، فيتم من خلالها جرائم القرصنة والهجمات على الاتصالات الالكترونية والمحادثات الموجودة في الأنظمة الالكترونية ، ومن الصور البسيطة لهذه الجرائم أيضاً ، جرائم الدخول أو البقاء غير المشروع إلى الأنظمة المعلوماتية خصوصاً إذا صاحب ذلك محو أو تغيير أو تخريب للمعطيات الموجودة في النظام ، ويتم ذلك من خلال الوصول إلى المعلومات والبيانات المخزنة في أنظمة المعلومات الالكترونية، كما وتتم الاعتداءات على الاتصالات والمحادثات الالكترونية من خلال عرض رسالة الكترونية ، أو الاستماع بشكل غير قانوني إلى محادثة الكترونية، و لا يلزم أن تحتوي الرسالة أو المحادثة على معلومات سريَة تتعلق بكلا طرفي الرسالة أو المحادثة ، فالحماية الجزائية تشمل المراسلات و المحادثات الخاصة ، بغض النظر عن مضمونها ، أي إذا ما كانت تحتوي على معلومات سرية أم لا، وبهذا الإطار فإنه هناك ثلاثة أنواع من الحماية وهي[60]:

- حماية الاتصالات وادارتها ونقلها بشكل صحيح .
- حماية ملكية الرسائل من الناحية المادية.
- حماية الرسائل من حيث محتوى الرسالة بما في ذلك حماية السرية الشخصية.

كما تعد الفيروسات من الوسائل التي لها مخاطرها على الخصوصية ، وذلك باعتبار أن الفضاءالرقمي بات أكثر المجالات تأثيراً في تطوير البئية التكنولوجية، وقد نتج عن ذلك إدخال الانترنت والتقنيات الحديثة في العديد من القطاعات مثل الحكومة الالكترونية والتجارة

[59] طوني عيسى، التنظيم القانوني لشبكة الانترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية، منشورات الحلبي الحقوية، بيروت ،2001 ، ص 169

[60] بيومي محمد حجازي ،مرجع سابق ، ص 25

الالكترونية، وذلك بأن الفيروسات يمكن أن تشكل خطراً كبيراً على الخصوصية لانها تسمح بالوصول غير المصرَح به إلى المعلومات الشخصية المخزنة على أجهزة الكمبيوتر ، مثل كلمات المرور والمعلومات المالية والتفاصيل الشخصية ، فالفيروسات برامج تكرر نفسها على نظام الكمبيوتر، ويمكنها أن تقضي على جهاز الكمبيوتر أو تعطّله أو تحدث به خللاً،وتأتي بأشكل وأحجام مختلفة، وبعضها ليست خطيرة ولكنها مزعجة ، ويتم كتبتها باستخدام إحدى لغات البرمجة منخفضة المستوى لإحداث تأثيرات مدمرة،[61] وهي تصيب أجهزة الكمبيزتر دون علم المستخدم لانها مصصمة لإلحاق الضرر بجهاز الكمبيوتر والتحكم فيه،والأوامر المكتوبة في هذه الفيروسات هي أوامر تقتصر على أوامر التخريب التي تلحق الضرر بنظم المعلومات أو البيانات.[62]

من خلال ما سبق يتضح أنه للحماية من مخاطر انتهاك الخصوصية في الفضاء الرقمي ، من المهم اتخاذ إجراءات آمنة في التصفح ، وتوخي الحذر من الراوبط والمرفقات المشبوهة ، واستخدام كلمات مرور قوية ، واستخدام برامج مكافحة الفيروسات باستمرار، وتطوير وسائل حماية الخصوصية الرقمية لمواجهة التطور والتحديات المتجددة.

**الفرع الثاني: الجريمة الالكترونية والاعتداء على الخصوصية الرقمية**

نتيجة للتطور في عالم المعلومات تعدد الجرائم وتطورت وتنوعت وازدادت، كما نشأت أنواع جديدة من الجرائم التي ظهرت بظهور أجهزة الكمبيوتر ، وقد اتخذت هذه الجرائم مظاهر مختلفة، وأصبحت تشكل خطراً حقيقياً على جميع الأصعدة الاقتصادية والاجتماعية والقانونية ، كخطر عمليات القرصنة على الاستثمارات والعمليات المالية وغيرها، كما أن مرتكبوا هذه الجرائم يختلفون عن مرتكبي الجرائم التقليدية ، لأنهم في الغالب أشخاص على مستوى عالٍ من الخبرة والمعرفة في مجال المعلوماتية ، وقد يكون بعضهم من صغار السن ، مما يجعل طبيعة تلك الجرائم يخرج عن مسار الجريمة التقليدية أو المجرم العادي ، كما أن الإثبات الجنائي للأدلة الرقمية يعد من أبرز التطورات في الوقت الحاضر ، وعند تناول تعريف الجريمة الالكترونية فقد تم تعريفها بأنها : "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو التي تحوَل عن طريقه" ، كما تم تعريفها بانها : "كل سلوك غير

---

61 أمير فرج يوسف ، الجرائم المعلوماتية عبر شبكة الانترنت، دار المطبوعات الجامعية ، الإسكندرية ، 2008، ص 62

62 عمرو عيسى الفقي، الجرائم المعلوماتية ، جرائم الحاسب الآلي والانترنت في مصر والدول العربية، المكتب الجامعي الحديث، الإسكندرية، 2006، ص230

مشــروع أو غير مســموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات " ، أو هي " نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطاً بتقنية المعلومات "، كما وجدت تعريفات متعلقة بوسيلة ارتكاب الجريمة أي كل فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية ، أما تعريف جريمة الكمبيوتر فهي : " كل سلوك غير مشروع معاقب عليه قانوناً وصادر عن إرادة جرمية ومحله معطيات الكمبيوتر "، فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشورعية تنفي عن الفعل الصفة الجرمية ، ومعاقب عليه قانوناً في عدة دول لأن إسباغ الصفة الجرمية لا يتحقق إلا بإرادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفاً للأخلاق العامة .[63]

وبتناول أركان هذه الجريمة فإن الأركان الثلاثة لهذه الجريمة ،هي الركن المادي والمعنوي والشرعي.

فالركن المادي ترتبط طبيعته في الجرائم الإلكترونية بالمشكلات المُثارة، ويقصد بذلك سوء استخدام الأنظمة الإلكترونية بطريقة غير مشروعة، أو اقتحام أي آثار مادية ملموسة تساهم في تدمير المعلومات، أو السرقة لبطاقات الائتمان أو التزوير والتلاعب في البيانات المرتبطة بالحواسب الآلية ، ويعتبر السلوك الإجرامي عنصراً أساسياً في الركن المادي في الجرائم التقليدية، كمشاهدة الجاني ورؤيته رؤية العين في قيامه بالقتل أو السرقة أو التزوير، أمّا في الجرائم الإلكترونية فيكون من الصعب أن يتم ارتكاب أو امساك الجاني مادياً، وذلك لأنَّها عبارة عن جرائم يتم ارتكابها من خلال المعلومات المتوافرة عن الحاسبات الآلية.

أما الركن المعنوي فيقصد به الحالة النفسية لمرتكبي الجرائم الإلكترونية، مع أهمية التركيزعلى العلاقات التي تكون مرتبطة ما بين ماديات الجريمة وشخصية الجاني. وفيما يتعلق بالركن الشرعي فهو الصفات غير المشروعة للفعل ، إذ يكون هنالك قاعدة للتجريم ، وعقوبات مفروضة على الجرائم المرتبطة بأنظمة المعلومات أي الجرائم الالكترونية، ويكون السلوك الأجرامي أيضاً مرتبطاً بأنظمة المعلومات ومرتبطاً أيضاً بالمعلومات المخزنة، أو التي يتم إدخالها، إذ قد يتمثل أيضاً في تدمير النظام المعلوماتي أو التزوير، وذلك من خلال التسلل إلى أرصدة الحسابات المتوافرة في البنوك ، أو أية معلومات أخرى.[64]

---

[63] نهلا عبد القادر المومني، مرجع سابق، ص 50

[64] شهاب ، بن حامد المسعود ، أركان الجريمة الالكترونية ،المجلة الدولية للبحوث والدراسات القانونية، المملكة العربية السعودية ، 2022.

أما عن دور الكمبيوتر في الجريمة الالكترونية فيلعب الكمبيوتر عدة أدوار في ارتكاب الجرائم ، ودوراً رئيسياً في اكتشافها ، فقد يكون هدفاً للجريمة وذلك كما في حالة الدخول غير المصرح به إلى النظام أو هجمات الفيروسات لتدمير الملفات المخزية والبيانات أو تعديلها ، أو في حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر الأنظمة ، كذلك يكون الكمبيوتر هدفا للجريمة عندا يتم الاعتداء على سرية المعلومات وخصوصيتها ، أي أن توجه هجمات الكمبيوتر إلى المعلومات بقصد المساس بالسريَة أو المحتوى ، أو تعطيل القدرة والكفاءة للأنظمة للقيام بعملها ، ويكون هدف هذا النشاط الإجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله أو المساس بسلامة المعلومات ، وقد يكون الكمبيوتر أداة للجريمة لارتكاب جرائم تقليدية ، كاستغلال الكمبيوتر للاستيلاء على الأموال وبطاقات الائتمان ، أو استخدام تقنيات التزييف والتزوير ، وقد يستخدم أيضا كوسيلة في جرائم القتل، والتلاعب ببرمجة قواعد البيانات ، بالإضافة الى ما سبق قد يكون الكمبيوتر بيئة الجريمة ، كتخزين البرامج التي تستخدم للقرصنة ، أو لترويج الوسائل غير المشروعة.[65]

وبقراءة نصوص التشريعات العربية ؛ تلاحظ الباحثة أنه لم يتم وضع تعريف واضح للجريمة الالكترونية بشكلٍ مباشر .

فيما يتعلق بالمشرع الفلسطيني لم يتطرق إلى تعريف واضح للجريمة الالكترونية كونها جريمة حديثة، لكن في قرار بقانون رقم 10 لسنة 2018 نص القرار في المادة (12 ) والمواد( 1- 5) ، على طبيعة المعلومات المشمولة بالحماية الجزائية [66]، وهي على سبيل المثال :

1- بطاقات التعامل الالكتروني .
2- أموال وبيانات الغير
3- جرائم الحاسب الآلي.
4- الجرائم المرتبطة بالذمة المالية.
5- بطاقات الائتمان.

أما المشرع الأردني لم يتناول تعريفاً للجريمة الالكترونية في قانون جرائم أنظمة المعلومات الأردني رقم 30 لسنة 2010، أما فيما يتعلق بالطبيعة القانونية للمعلومات المشمولة بالحماية الجزائية هنا ، فيتمحور الحديث عن الوضع القانوني للبرامج والمعلومات ، وهل لها قيمة في ذاتها أم أنها مجموعة من القيم القابلة للاستثناء ويمكن الاعتداء عليها بأي طريقة كانت؟

[65] المومني ، نهلا عبد القادر، المرجع السابق ، ص 46
[66] انظر المواد 1-5 و مادة 12 من القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018 – تشريع فلسطيني

ولقد انقسم الفقه إلى اتجاهين:

- الأول : يرى أن الأشـياء المادية وحدها هي التي تقبل الحيازة والاسـتحواذ ، وأن الشـئ موضـوع السـرقة أو الاعتداء يجب أن يكون مادياً له كيان ملموس، ولما كانت المعلومات ذات طبيعة معنوية وغير قابلة للحيازة أو الاســتحواذ إلا من خلال حقوق الملكية الفكرية لذا تستبعد المعلومات من موضوع السرقة مالم تكون مسجلة على أسطوانة أو شريط.
- الثاني: هناك اتجاه يرى أنه يجب التفرقة بين المال المعلوماتي المادي ، حيث أنه لايمكن أن يخرج عن هذه الطبيعة مثل آلات وأدوات الحاسب الآلي، مثل وحدة العرض البصـري ، ووحدة الإدخال ، وأن هناك من المال المعلوماتي ما يشـتمل على مضـمون معنوي وهو الذي يعطيه القيمة الحقيقية ، وهي المال المادي مثل الشــريط الممغنط ، أو الأســطوانة الممغنطة أو الذاكرة أو الســلك التي تنقل عبرها الأشــارات عن بعد، كما هو الحال في جرائم التجسس عن بعد .

إذن فإنه إذا حدثت سرقة فإنه لا يسرق المال المسجل عليه المعلومة أو البرامج لقيمته المادية وهي ثمن الشريط ، أو ثمن الأسطوانات ، وإنما ما يسرق هو ما يسجل عليها من معلومات وبرامج.[67] ويعتبر تحديد المعلومات التي يجب حمايتها تحت مظلة القانون الجزائي شـيء مسـتحيل، حيث من الصــعب حصــر هذه المعلومات أو البيانات ، فتتشــعب وتتعدد أنواع المعلومات مما يجعل من الصــعب تحديدها ، وتكمن الصــعوبة الأكبر فيما هو مباح نشــره وتداوله وما هو محظور نشــره وتداوله.

وقد جاء في القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية الفلسطيني ، ذكر العديد من المعلومات والبيانات المشمولة بالحماية الجزائية [68]، منها على سبيل المثال :

1- استغلال تواقيع الغير عن طريق استخدام أدوات إنشاء التوقيع الالكتروني المتعلقة بتوقيع شخص آخر وهذا في المادة 8 من القرار بقانون.
2- البيانات المتعلقة بهوية الأشــخاص أو إصــدار شــهادات مزورة ، م (10 ) من القرار بقانون.
3- المستندات الرسمية الإلكترونية أو مستندات الدولة أو الهيئات أو المؤسسات العامة ، المادة (11) من ذات القرار بقانون.

[67] جلال محمد الزعبي ، أسامة محمد ، جرائم تقنية نظم المعلومات الالكترونية ، دار الثقافة، عمان، ط1، الإصدار الرابع ، 2013 ،ص 36،37.
[68] انظر المواد 8، 10، 11،21 من القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية الفلسطيني .

4- البيانات المتعلقة بتنظيم نقل وزراعة الأعضاء البشرية عن طريق إنشاء مواقع الكترونية بقصد الاتجار بالأعضاء البشرية.

5- البيانات المتعلقة بحرية الصحافة والطباعة والنشر وحقوق الملكية الفكرية ، المادة 21 من القرار بقانون.

جدير بالذكر بأن تحديد البيانات الشخصية دائماً ما يصاحبه صعوبة مطلقة لما لهذه البيانات من تنوع وتشعبات متعددة ، ومن الصعب حصرها.

فالمشرع المصري قد عرف البيانات الشخصية في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، بأنها :" أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.[69]

كما عرف قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020 البيانات الشخصية بأنها :" أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات أو أي بيانات أخرى كالاسم، أو الصوت، أ, الصورة ، أو رقم تعريفي ، أو محدد للهوية عبر الانترنت ، أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية، أو الثقافية أو الاجتماعية."[70]

وباستقراء النصوص القانونية في المشرع المصري ، فإن قانون حماية البيانات المصري وقانون مكافحة تقنية المعلومات أورد التعريفات المتعلقة بالبيانات الشخصية للأفراد ، ونظم استخدام المعلومات وتداولها، كما نص على حماية الحقوق المتعلقة بالمعلومات، وتعزيز الشفافية والمساءلة في التعامل مع المعلومات الشخصية ، لكن لا زالت هذه التشريعات بحاجة إلى تحديد واضح ومفصل في القضايا المتعلقة بحماية الخصوصية الرقمية ، لغايات سد الثغرات الموجودة في تلك التشريعات.

من خلال ما سبق ترى الباحثة أن حماية البيانات أو المعلومات الشخصية تعد حقاً أساسيا للجميع، لكنهم يشعرون دائماً بالسيطرة على بياناتهم الشخصية أو استغلالها ، وأنها غير مشمولة بالحماية الكاملة التي تجعله مطمئنين عليها، حيث أن أحد نتائج عصر التحول الرقمي والتطور التكنولوجي هو أن الخصوصية الشخصية تتآكل بسرعة، حيث كشفت قواعد البيانات والمعلومات وشبكات الكمبيوتر وتقنيات التخزين عن الكثير من الأشخاص حول العالم ممن يتعرضون لتهديدات المراقبة والسيطرة السلبية .

---

[69] المادة رقم 1 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 ، تشريع مصري.

[70] قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

**المطلب الثاني : خطورة أنظمة المعلومات على الحياة الخاصة وعوامل الاعتداء المعلوماتي على الخصوصية**

في الوقت الحاضر ، أصبح استخدام الانترنت يعرض المستخدمين له إلى الكثير من المخاطر، وقد دار الكثير من النقاش حول مخاطر وسائل التكنولوجيا الحديثة على جميع جوانب الحياة الشخصية وخصوصيتها، نظراً لما يتطلبه من الإدلاء ببعض البيانات والمعلومات الشخصية مثل الاسم والعنوان ، وتفصيل حول الحساب المصرفي ، والعادات اليومية وأسماء الأشخاص ، بل و أكثر من ذلك ، فشبكة الانترنت أصبحت تربط الجميع بطريقة متناسقة ، وأصبحت مرتبطة بجميع جوانب الحياة من خلال جمع وتخزين ونشر المعلومات ، مما يستلزم أن أي اعتداء على المعلومات الشخصية على الانترنت هو اعتداء على الخصوصية ، وعلى هذا الأساس ستتطرق الباحثة في هذا المطلب إلى تناول مدى خطورة أنظمة المعلومات على الحياة الخاصة من خلال الفرع الأول ، وإلى عوامل الاعتداء المعلوماتي على الخصوصية من خلال الفرع الثاني لهذا المطلب.

**الفرع الأول : خطورة أنظمة المعلومات على الحياة الخاصة**

لا ينكر أحد ما للحق في الخصوصية من أهمية للفرد والمجتمع على حد سواء، فهو صمام الأمان الذي يحفظ للفرد استقرارة النفسي، والشعور باحترام أسراره ، ويصبح ضميره يقظا بما من شأن ذلك أن يسهم في تطور مجتمعه وهذا كله يعود بالنفع على الفرد والجماعة.[71]

ومن الثابت أن نطاق حماية الحياة الخاصة للأفراد يوجب أن يظل هذا النطاق بعيداً عن تدخل الغير وعن العلانية، وعليه يدخل في نطاق الحماية الخاصة البيانات الشخصية، ذلك أن الصلة وثيقة جدا بين الحق في الخصوصية والحق في حماية البيانات الشخصية، التي تدخل في صميم الحياة الخاصة للأفراد.[72]

وعندما يستخدم الأفراد مواقع الانترنت فإنهم يتوقعون قدراً من السرية والخفية في نشاطهم أكثر مما يتوقعون في العالم المادي الواقعي ، ففي العالم المادي يمكن ملاحظة وجودهم ومراقبتهم من قبل الآخرين، ويعتقد الفرد أن عدم الكشف عن بياناته تكون غير متاحة لأحد أن يعرف من هو أو ماذا يفعل ، لكن الفضاء الرقمي جعل العديد من التحديات الجديدة في مواجهة حماية الفرد وحماية الخصوصية، فأنظمة المعلومات تزيد كمية البيانات المجمعة و المعالجة والمنشأة ، إذ أن الانترنت

[71] د. أحمد فتحي سرور، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، عدد 54 ، ص 35.
[72] يحيى صقر، حماية حقوق الشخصية في إطار المسؤولية التقصيرية " دراسة مقارنة" ، رسالة دكتوراه

يتجه إلى جمع البيانات في العالم الحقيقي لتصـــبح أكثر ســـهولة في الفضـــاء الرقمي من حيث الوصـول إليها، وأكثر ملائمة لحوسبتها ، وبالتالي تصبح أسـهل لتبادل المعلومات بكافة أشكالها ، عبر تقنيات التصـــفح والبرمجة والنقل ، كذلك فإن أنظمة المعلومات أتاحت عولمة المعلومات والاتصـــالات عبر الحدود دون أي اعتبار للجغرافيا والســـيادة ، بالتالي الأفراد يفصـــحون عن معلوماتهم الخاصـــة لجهات داخلية وخارجية ، وجهات ليس لها مكان معروف، وهذا ما يؤدي إلى مخاطر إســـاءة اســـتخدام البيانات الخاصـــة على وجه الخصـــوص في البلدان التي لاتتوفر فيها مستويات لحماية الحق في الخصـوصـية، كما تتجلى بشـكل واضـح الخطورة على الحياة الخاصـة عبر الفضـــاء الرقمي في تقنية التجســـس عبر الانترنت ، و هذا الأمر يزداد خطورة إذا قامت الحكومات بذاتها بالتجسس على مراسلات الأفراد وخصوصياتهم، عن طريق التنصت أو الرقابة الالكترونية، في ظل اســـتخدام ما يعرف بالحكومات الالكترونية، ولكن تشـــير وجهات النظر أنه يجوز تخزين البيانات بقدر معين ونوعية معلومات معينة للمصلحة العامة التي تكون مباح المساس بها عن طريق تخزينها ومعالجتها ، والبعض يرى ان ذلك يؤدي إلى اختلال التوازن المطلوب بحيث تسيطر السلطات في الدولة على المعلومات الخاصة المخزنة للأفراد.[73]

وقد سـبق وأن تم الذكر أن التشـريعات العربية لم تضـع جميعها تنظيماً قانونياً واضـحاً وشـاملاً لحماية البيانات الشخصية، ويجب تنظيم استخدام الحاسبات الآلية والشبكات من خلال التشريع أي القانون ، ولا يجب أن يترك ذلك إلى اللوائح التي تصـدر عن السـلطة التنفيذية، لأن التشـريع هو المعبر عن إرادة الشـعب ، ففي فلسـطين أقر القرار بقانون رقم 10 لسـنة 2018 بشـأن الجرائم الالكترونية بموجب مرسوم رئاسي ، ولكن هذا القانون لم ينصف الصحفيين حيث لاقى معارضة شديدة من قبل النشطاء والصحفيين والمجتمع المدني الفلسطيني ، نظراً لتضمنه بنوداً فضفاضة ، من شأنها أن تهدد حرية التعبير، وتهدد الحق في الخصوصية على الانترنت.[74]

وفي عام 2019 اصدر مجلس الوزراء الفلسطيني في رام الله القرار رقم 3 لسنة 2019 الخاص بحماية البيانات الشـخصـية الخاصـة بالمواطنين الفلسـطينيين ، وقد جاء في نص المادة (1) من القرار أنه :" يحظر استخدام البيانات الشخصية ( المباشرة \ غير المياشرة) الخاصة بالمواطنين متلقي الخدمة من الشركات والمؤسسات المزودة بها لأغراض تجارية ، دون الحصول على إذن مسبق منهم تحت طائلة المسؤولية القانونية " .[75]

---

[73] عمر أحمد حسبو، مرجع سابق، ص92.

[74] انظر المادة 22 من القرار بقانون رقم 16 لسنة 2017 بشأن الجرائم الالكترونية ، بموجب مرسوم رئاسي فلسطيني .

[75] انظر القرار رقم 3 لسنة 2019 الخاص بحمياية البيانات الشخصية الخاصة بالمواطنين الفلسطينيين.

على الرغم من أن نص هذه المادة يوفر الحماية المتعلقة بالبيانات الشـــخصـــية المتعلقة بالمواطن الفلسطيني إذا تم استغلالها من قبل الشركات المزودة للخدمات لأغراض تجارية إلا أنه يجب وكما أسلفنا سابقاً ، أن تصدر قوانين منظمة من قبل التشريع وليس عن طريق السلطة التنفيذية.

وفيما يتعلق بأثر أنظمة المعلومات على الحياة الخاصـــة في مصـــر فترى الباحثة أن الدســـتور المصـــري تناول مفهوم الحق في الحياة الخصـــوصـــية في أكثر من موضـــوع، حيث اســـتعرض الجوانب المتعلقة بخصـوصـية مسـتخدمي وسـائل التواصـل الاجتماعي من جانب ، بالإضـافة إلى بعض النصـــوص التي نحدثت عن الضـــمانات المتعلقة بالإجراءات الواجب اتباعها أثناء تفتيش المنازل والأفراد.

فقد تضـمنت المادة (57) من الدسـتور المصـري الصـادر عام 2014 ما يلي : " للحياة الخاصـة حرمة، وهي مضـــمونة لا تمس، وللمراســـلات البريدية والبرقية والالكترونية والمحادثات الهاتفية وغيرها من وسـائل الاتصـال حرمة، وحمايتها مكفولة ،ولايجوز مصـادرتها أو الاطلاع عليها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي بينها القانون."[76]

وأيضـا أصـدر المشـرع المصـري قانون مكافحة جرائم تقنية المعلومات رقم 175 لسـنة 2018، حيث أفرد المشرع المصري فصلاً مستقلاً لتجريم أفعال مختلفة يشكل كل منها اعتداءاً على الحياة الخاصة تحت مسمى "الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي الغير مشروع".[77]

كما أقر المشـرع في العام 2020 ، القانون المصـري لحماية البيانات الشـخصـية ، ويهدف هذا القانون إلى وضع إطار تشريعي يكفل للمستخدمين حماية بياناتهم الشخصية التي تخضع للمعالجة الإلكترونية، كما يخاطب القانون الشـركات والمؤسـسـات التي تتعامل مع قواعد البيانات الخاصـة بالمســـتخدمين ويحدد العلاقة التي تحكم بين الأطراف ومعاييرها ، كما نص القانون على إنشـــاء مركز لحماية البيانات الشـــخصـــية لتكون مهمته الرقابة على تنفيذ القانون ، وقد جاء هذه القانون محاكياً للمعايير والقوانين العالمية كاللائحة الأوروبية لحماية البيانات ، ورأت عدة جهات أن القانون بحاجة للأخذ بعين الاعتبار عدة مبادئ أساسية لتتواءم مع الاتفاقيات والمعايير الدولية.[78]

---

[76] المادة 57 من الدستور المصري لسنة 2014.

[77] انظر المواد 25 ،26 من قانون مكافحة جرائم تقنية المعلومات رقم 176 لسنة 2018، جمهورية مصر العربية ، " صور وأشكال الاعتداء على الحياة الخاصة "

[78] الاء كليب ، قانون حماية البيانات المصري في ضوء المعايير الدولية ، مؤسسة ا حرية الفكر والتعبير ، القاهرة ، 2021 ، ص 11.

أما المشرع الأردني ، بالنظر إلى نص المادتين (21،23) من قانون الاتصالات الأردني رقم 13 لسنة 1995 ، نجد أنها أتاحت للوزارات والدوائر الحكومية إنشاء وتشغيل شبكات اتصال خاصة فقد نصت المادة 21[79] من القانون على أن:

أ- للوزارات والدوائر الحكومية والمؤسسات العامة إنشاء وتشغيل شبكات اتصالات خاصة بها دون الحصول على تصريح بذلك ، باستثناء الأحكام المعلقة باستخدام الموجات الراديوية، على أن يتم اعلان الهيئة خطياً بذلك.

ب- لمجلس الوزراء بناء على تنسيب من الهيئة استثناء أشخاص اعتباريين من شروط الحصول على تصريح إنشاء وتشغيل شبكات اتصالات خاصة .

وتنص المادة ( 23 ) من ذات القانون على أنه : "يجوز إنشاء شبكة اتصالات وتشغيلها دون تصريح أو ترخيص إذا كانت تلك الشبكة مخصصة للربط بين أجزاء العقار الواحد أو العقارات المتجاورة ، إذا كانت العقارات مملوكة أو مشغولة من قبل شخص واحد، على أم يتم الحصول على موافقة الهيئة عند ربط هذه الشبكة مع شبكة الاتصالات العامة أو أي شبكة خاصة أخرى".[80]ومن خلال تلك النصوص نجد أن الصلاحيات المخولة للحكومة والمؤسسات العامة يجب أن تكون مقيدة وتحقق المصلحة العامة دون المساس بحياة الأفراد الخاصة[81] ، مع الأخذ بعين الاعتبار العقوبة التي فرضها المشرع في المادة (355 ) من قانون العقوبات الأردني [82] التي تنص على أنه : يعاقب بالحبس مدة لاتزيد على ثلاثة سنوات كل من :

1-حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية أباح هذه الأسرار لمن ليس له صلاحية الاطلاع عليها ،أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع للمصلحة العامة.

2-كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقتضي ذلك طبيعة وظيفته.

3-كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع.

هذا وإن جل التشريعات العربية لم تجد قانون شامل وموسع لحماية البيانات الشخصية، الأمر الذي يدفع إلى ضرورة إنشاء قوانين شاملة وواضحة فيما يخص الحماية الجزائية للخصوصية في العصر الرقمي، نظراً للتقدم الحاصل حيث بات من السهل اختراق البيانات الخاصة بالأفراد،

---

[79] قانون الاتصالات الأردني رقم 13 لسنة 1995

[80] قانون الاتصالات الأردني، مرجع سابق، م 23

[81] بارق منتظر اللامي، مرجع سابق ، ص 33

[82] قانون العقوبات الأردني رقم 16 لسنة 1960، المادة 355

وانتهاك الخصوصية عبر وسائل التواصل الاجتماعي والشبكة الالكترونية، كما يطرح التساؤل حول الضمانات الواجب اعتمادها لحماية لحياة الخاصة للأفراد، والإجراءات الواجب اتباعها من أجل حصرها في القطاع العام المخول قانوناً بتجميع البيانات الخاصة للأفراد وفقاً للقانون ، لتجنب تعرض الأفراد لتبادل بياناتهم الخاصة من مؤسسة إلى أخرى دون وجود أي ضوابط تحمي خصوصية الفرد وبياناته ومن الممكن أن تهدم حياة الفرد وبكل سهولة.

**الفرع الثاني : مبررات الاعتداء المعلوماتي على الحياة الخاصة**

تشير خصوصية البيانات والمعلومات إلى حماية المعلومات الشخصية من الوصول غير المصرح به ، أو الاستخدام أو الكشف أو الاتلاف ، ويتضمن ذلك ضمان سيطرة الأفراد على معلوماتهم الشخصية ، وأن تكون المؤسسات والشركات تتسم بالوضوح والشفافية بشأن كيفية جمع البيانات واستخدامها ومشاركتها مع أطراف أخرى ، فإن تخزين البيانات حتى ولو كان برضا الفرد المعني ، لا يعني أن هذه البيانات قابلة للتداول ، ولا يعني كذلك أنها انتقلت من حالة الخصوصية إلى حالة العلانية عن طريق الاطلاع عليها من قبل كبير من الأشخاص العاملين في مجال المعلوماتية ومزودي الخدمة أو الجهات الرسمية، ومن ثمَ تنتهك سريتها وتتعرض للإفشاء ، وقد تصل في أحيان كثيرة إلى ابتزاز الشخص الذي تتعلق به تلك المعلومات.[83]

كما أن انتهاك الخصوصية لا ينحصر في الكشف عن المعلومات أو البيانات الشخصية فقط ، بل يشمل تدميرها وإتلافها وإفقادها قيمتها بشكل كلي أو جزئي ، وذلك من خلال استخدام الفيروسات التي تؤدي إلى إتلاف جميع المعلومات أو إتلافها بشكل جزئي ، أو إحداث خلل في الجهاز الحامل للمعلومات ، وبذلك يتحقق فعل الانتهاك الذي يعاقب عليه القانون.

هذا وتشير معظم التشريعات بأن المساس بأنظمة المعالجة الآلية للمعطيات يكون في الحالات التالية:[84]

- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات ويتمثل في الصورة البسيطة المتمثلة في مجرد الدخول أو البقاء غير المشروع ، كالدخول إلى نظام الشبكة الخاص بمؤسسات أو منظمات دون الإذن الصريح، وهذا يؤدي إلى الوصول إلى البيانات الخاصة بالعملاء الخاصين بتلك المنظمة أو المؤسسة، كما يتمثل في الصورة المشددة وتكون

[83] محمد أمين الشوابكة، مرجع سابق ، ص 134

[84] عبد الفتاح بيومي حجازي ، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للاصدارات القانونية، القاهرة، 2011 ، ص492

في حالة ما إذا نتج عن الدخول أو البقاءغير المشـروع تغيير أو محو في المعطيات الموجودة في النظام أو تخريب لنظام تشـــغيل منظومة معلوماتية ، كالتلاعب في البيانات الخاصـــة بمؤسـسـة أو شـركة أو نقل هذه البيانات إلى طرف آخر ، مما يشـكل تهديداً على خصـوصـية العملاء .

إذ نصت المادة 4 من القرار بقانون الجرائم الإلكترونية الفلسطيني الجديد رقم (10) لسنة 2018 على أنه "

1. كل من دخل عمداً دون وجه حق بأية وسيلة موقعاً الكترونياً، أو نظاماً، أو شبكة إلكترونية، أو تجاوز الدخول المصرح به، أو استمر في التواجد بها بعد علمه بذلك، يعاقب بالحبس أو بغرامة لا تقل عن مائتي دينار أردني ولا تزيد على الف دينار أردني أو بالعقوبتين كلتيهما.
2. إذا أرتكب الفعل المحدد في الفقرة (1) من هذه المادة على البيانات الحكومية، يعاقب بالحبس لمدة لا تقل عن ستة شهور أو بغرامة لا تقل عن مائتي دينار ولا تزيد على ألف دينار أردني أو بالعقوبتين كلتيهما." [85]

ويلاحظ أن المشرع الفلسطيني توسع بالحديث عن طبيعة النشاط الواقع على البيانات والمعلومات من حيث الحذف والنسخ والنشر أو التعديل أو انتحال شخصية المالك، حيث اعتبر المشرع أن هذه الجرائم من الجنايات، بل وتشدد بالعقوبة في حال نتج عن الدخول غير المصرح نسخ أو حذف أو تعديل أو نشر لبيانات حكومية، والعلة من ذلك خطورة هذه الجرائم على الأمن العام في الدولة وعلى النظام العام داخل المجتمع.[86]

- الاعتداءات العمدية على نظام المعالجة الآلية ويكون من خلال أي هجوم أو اعتداء متعمَد على البيانات، كالحذف والتعديل وإدخال بيانات ، ولايشـترط الجمع بن تلك الأعمال بل يكفي أن يتوفر أحدها فقط حتى يتوفر الركن المادي ، كأن يدخل موظف في شـــركة إلى قاعدة بيانات بحذف بعص البيانات للزبائن بهدف إلحاق الضرر بالأفراد أو الشركة.
- استخدام البيانات كوسيلة لارتكاب الجرائم الماسة بالمعلوماتية ويحدث ذلك من خلال بحث أو تصميم أو تجميع أو تخزين أو نشر أو متاجرة في المعلومات المخزنة أو المعالَجة أو المنقولة من خلال النظام الالكتروني ، كأن يتم الدخول إلى نظام معلوماتي ويقوم بجمع بيانات خاصـة حول الأفراد أو الزبائن بغرض بيعها أو مسـاومة أصـحابها وابتزازهم بها ،وهذا الاسـتخدام يجب أن يكون متعمداً أو احتيالياً بنية الغش حتى يتوفر القصد الجنائي.

[85] انظر قرار بقانون الجرائم الالكترونية الفلسطيني رقم 10 لسنة 2018
[86] عبد الله ، ذيب محمود، جريمة الدخول غير المشروع ، جامعة الاستقلال ، فلسطين ، 2018، ص 10

وقد خصص المشرع المصري الفصل الأول من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 ، لجرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات، حيث جرم جرائم الدخول غير المشورع والبقاء بدون وجه حق على البيانات الشخصية ، على غرار المشرع الفرنسي و المشرع الفلسطيني ، فقد قضت تلك التشريعات بالمسؤولية الجزائية عن تلك الجرائم .[87]

[87] د. أحمد، براك ، المرجع السابق ، ص 263.

## المبحث الثاني : وسائل حماية الخصوصية في العصر الرقمي

بدايةً لا بد من توضيح المقصود بأمن المعلومات ومدى أهميته؛ حيث أنه عبارة عن مجال حيوي وحاسم في العالم الرقمي الحديث، ويعنى بحماية المعلومات والبيانات من أي تهديد أو مخاطر قد تتعرض لها في بيئة الانترنت والتكنولوجيا الرقمية، ويعتبر أمن المعلومات عملية ذات أهمية بالغة نظراً للتزايد الكبير في كم المعلومات التي يتم تخزينها ومعالجتها عبر شبكات الانترنت والأنظمة التكنولوجية.

وتكمن أهمية أمن المعلومات في حماية البيانات والخصوصية في العصر الرقمي، حيث أن أهمية أمن المعلومات لا تقتصر فقط على الشركات والمؤسسات بل أنها تمتد إلى كافة جوانب الحياة اليومية.

في هذا المبحث سيتم تناول الوسائل التنظيمية لحماية البيانات الشخصية في المطلب الأول، وفي المطلب الثاني توضيح الوسائل التقنية لدورها المحوري في حماية الحق في الخصوصية الرقمية.

### المطلب الأول : الوسائل التنظيمية لحماية البيانات الشخصية

لقد أصبحت حماية البيانات الشخصية ذات أهمية متزايدة في العصر الرقمي اليوم ، مع التقدم السريع في التكنولوجيا والاستخدام الواسع النطاق للإنترنت، يشارك الأفراد باستمرار معلوماتهم الشخصية عبر الإنترنت وذلك بدءاً من منصات التواصل الاجتماعي وحتى مواقع التسوق عبر الإنترنت، حيث يتم جمع بياناتنا الشخصية وتخزينها واستخدامها من قبل كيانات مختلفة، غالباً دون موافقتنا أو علمنا الصريح ، وهذا يثير المخاوف بشأن الخصوصية ، والحاجة إلى اتخاذ تدابير فعالة لحماية معلوماتنا الشخصية.

إن أهمية حماية البيانات الشخصية تبدأ من أهمية المسؤولية الفردية لحماية بياناتهم ، حيث أنه يجب على الأفراد اتخاذ خطوات ووسائل احتياطية لحماية بياناتهم الشخصية ، وذلك يكون من خلال :

1- توخي الحذر بشأن المعلومات التي مشاركتها عبر الفضاء الرقمي ، وباستخدام كلمات مرور يصعب اختراقها ، بالإضافة إلى تحديث إعدادات الخصوصية على جميع الحسابات ، فهذه التدابير والخطوات تقلل مخاطر وقوع البيانات الشخصية والتطبيقات في خطر الاعتداء والانتهاك .

2- مما لا شك فيه بأن دور شركات التكنولوجيا ومزودي الخدمات في ضمان حماية البيانات هو دور محوري ورئيسي في تحمل مسؤولية تنفيذ تدابير أمنية واستخدام بروتوكولات وسياسات

حماية البيانات الشخصية ، وإعطاء الأولوية لخصوصية عملائهم ، والتحلي بالشفافية بشأن كيفية جمع البيانات الشخصية وتخزينها ومعالجتها .

3- النظر في دور التشريعات والأنظمة في حماية البيانات الشخصية واستخدامها، فلقد أدركت الحكومات في جميع أنحاء العالم الحاجة إلى قوانين شاملة لحماية البيانات لحماية خصوصية الأفراد، وتعد اللائحة العامة لحماية البيانات للاتحاد الأوروبي مثالاً بارزاً ، حيث تضع قواعد صارمة لكيفية جمع البيانات الشخصية ومعالجتها وتخزينها ، وتهدف هذه اللوائح إلى مساءلة المؤسسات عن حماية البيانات الشخصية ، ومنح الأفراد مزيداً من التحكم بمعلوماتهم الخاصة .

**المطلب الثاني: الوسائل التقنية لحماية البيانات الشخصية**

هناك وسائل مهمة لحماية البيانات الشخصية ، أصبح من الضرورة نشرها والاستفادة منها ، حيث أنها تساعد على حماية تبادل البيانات الحساسة والمهمة عبر الانترنت.

وفي هذا المطلب سوف تتناول الباحثة اثنتين من هذه الوسائل ، الأولى هي تقنية التشفير، والثانية هي تقنية المجهولية أو إخفاء الهوية .

**الفرع الأول : تقنية التشفير**

تقنية التشفير هي عبارة عن عملية تحويل البيانات السرية إلى صيغة غير قابلة للقراءة للأشخاص الغير مخولين، وتستخدم هذه التقنية في حماية البيانات الحساسة والمعلومات السرية من الاختراق أو الاستخدام غير المسموح به.

هذا ويعتبر التشفير أحد أهم الأدوات الأكثر فاعلية حالياً في مجال أمن المعلومات ، حيث بإمكان هذه التقنية حماية البيانات من القرصنة والتجسس والتلاعب ، ومع ظهور الجرائم الإلكترونية وانتهاك البيانات، أصبح الأفراد عرضة بشكل متزايد للوصول غير المصرح به وإساءة استخدام معلوماتهم الحساسة ، وهذا هو المكان الذي يتدخل فيه التشفير كأداة حاسمة في حماية البيانات الشخصية، ولقد ورد عدة تعريفات للتشفير في مجال المعلوماتية ، فقد عرف القانون الفرنسي تقنية التشفير: "جميع التقديمات التي ترمي بفضل بروتوكولات سرية إلى تحويل معلومات وإشارات غير مفهومة، أو القيام بالعملية المعاكسة ، وذلك عن طريق استخدام معدات أو برامج مهمة لهذه الغاية".[88]

[88] ورد هذا التعريف في الفقرة الأولى من المادة 28 من القانون الفرنسي رقم 90 -1170 الصادر بتاريخ 29 كانون الأول لسنة 1990، حول تنظيم الاتصالات عن بعد.

**- أهمية ودور التشفير في حماية البيانات الشخصية:**

أولا : حماية الخصوصية وضمان السرَية

حيث يعتبر التشفير من أهم الأدوات التي تحافظ على الخصوصية والسرية للمعلومات ، من خلال عدم السماح للأشخاص غير المخولين من الوصول إلى البيانات السرية وقراءتها، كذلك للتشفير دوراً حيويا في الحفاظ على خصوصية الأفراد من خلال جعل بياناتهم غير قابلة للفك لأطراف غير مصرح بها ، من خلال تشفير المعلومات الشخصية حتى لو تم اعتراضها أثناء الإرسال أو الوصول إليها دون إذن، فتظل عديمة الفائدة بالنسبة لمتسلسل ، فيوفر تشفير البيانات طبقة إضافية من الحماية ضد التنصت أو الاعتراض.

ثانيا: السلامة الرقمية

إذ يوفر التشفير طريقة آمنة لنقل البيانات ، سواء داخل الشبكات الداخلية أو غير شبكة الانترنت، فهو يحمي البيانات من التلاعب والتغيير غير المصرح به ، أي يضمن سلامة البيانات الشخصية من خلال تطبيق خوارزميات التشفير، فإن أي تعديلات يتم إجراؤ ها على البيانات المشفرة ستجعلها غير قابلة للقراءة وغير صالحة.

ثالثا : الحماية من الاختراق

من خلال استخدام التشفير يمكن الحد خطر الاختراق، والوصول غير المصرح به إلى البيانات الحساسة،وحتى حال وقوع اختراق لن يتمكن القراصنة من قراءة البيانات المشفرة.[89]

وتعتبر تقنية التشفير من أهم الأدوات التي توفر الأمن وسلامة المعلومات المتداولة عبر شبكة الانترنت ، على اعتبار أنها لا تقتصر فقط على حماية البيانات فحسب ، وإنما تشتمل على التحقق ومعرفة مرسل الرسائل ، والمصادقة على مضمونها، وعلى توقيع أصحابها الكترونياً عليها، والتحقق من سلامتها ، بالإضافة إلى ضمان عدم قابلية اختراقها.[90]

**الفرع الثاني: تقنية المجهولية وإخفاء الهوية**

لتحقيق التوازن بين فائدة البيانات والخصوصية، يمكن استخدام تقنيات إخفاء الهوية والتجميع ، حيث يتضمن إخفاء الهوية إزالة معلومات التعريف الشخصية من البيانات، مما يجعل من المستحيل ربطها مرة أخرى بفرد ما ، ومن ناحية أخرى، يتضمن التجميع الجمع بين البيانات من

---

89 انظر الموقع www.techcode.net

90 عبد الفتاح بيومي حجازي ، مرجع سابق ،ص 32.

عدة أفراد لإنشاء ملخصات إحصائية دون الكشف عن الهويات الفردية ، بحيث يمكن لهذه التقنيات حماية خصوصية الأفراد مع السماح في الوقت نفسه بالحصول على رؤى وتحليلات قيمة.

هذا وينظر الكثيرون إلى المجهولية على أنها حجر الزاوية في تعزيز حرية الرأي والتعبير والخصوصية على الإنترنت، ولكن يمكن أيضًا إساءة استخدامها للسيطرة على الأشخاص وإساءة معاملتهم.

يمكن للمستخدم إخفاء أو تمويه المعلومات المتعلقة بهويته الحقيقية، مثل الاسم الحقيقي والعمر والموقع واستخدامه للبيانات ، من خلال:

- إخفاء الهوية بالكامل بمعنى عدم الكشف عن أي معلومات تكشف هوياتهم/ن
- اخفاء الهوية جزئيا - الكشف عن معلومات التعريف الخاصة لجمهور محدود فقط لحمايتها من عامة الناس.

هناك طرق مختلفة متاحة لإخفاء أو تمويه معلومات الهوية الرقمية ، وهذه الأساليب تشمل الأدوات التقنية لإخفاء الهوية البرامج والمتصفحات والأنظمة المشفرة أو اللامركزية، كالشبكات الخاصة الافتراضية VPNالتي تخفي موقع المستخدم ، وتفاصيل الجهاز IP ، و طرق إخفاء الهوية التي تخفي الرابط بين الرسالة والمرسل ، والتشفير من طرق لآخر الذي يسمح للمرسل والمستلم فقط بفك تشفير المحتوى الرقمي .[91]

كما تتضمن الأساليب الأبسط لتحقيق المجهولية خلق هوية افتراضية بديلة، على سبيل المثال استخدام اسم مختلق "اسم مستعار" ، أو تمثيل افتراضي ("صورة رمزية") ، أو ملف شخصي مختلق ، ويمكن استخدام الهويات المتعددة كوسيلة لحماية الخصوصية ، أو يمكن استخدامها لهدف سيء كخداع المستخدمين الآخرين.[92]

---

[91] محمد الألفي، الحماية القانونية لقواعد البيانات في نظم المعلومات ، أعمال وندوات " مكافحة الجريمة عبر الانترنت"، المنظمة العربية للتنمية الإدارية ،2010، ص 194.

[92] المجهولية وتعدد الهوية الرقمية الموقع الالكتروني www.motoon.org

## الفصل الثالث

# التنظيم القانوني لحماية الحق في الخصوصية الرقمية في الاتفاقيات الدولية وفي ضوء المعايير الدولية والتشريعات المقارنة

بالرغم من اختلاف وجهات نظر الفقهاء في تحديد وضبط العناصر المكونة لفكرة الحياة الخاصة، إلا أن المشـرع في غالبية الدول قد أحاط تلك الخصـوصـية في حياة الأفراد بالحماية القانونية مع اختلاف درجات الحماية من تشـــريع لآخر، لذلك نجد أن كل القوانين العقابية قد جرَمت الأفعال والسلوكيات التي تعد انتهاكا على الحق في حرمة الحياة الخاصة ــ سواء كانت هذه الجرائم تقليدية أو تلك الجرائم التي ارتبطت بنظم المعلومات وتعد أعمالا جرمية مسـتحدثة يعاقب عليها القانون ، كما تضـافرت الجهود الدولية والإقليمية والوطنية في وضـع الإطار القانوني لحماية حقوق الأفراد وخصوصيته في العصر الرقمي.

ولذلك فقد حظيت حقوق الإنســـان بالاهتمام والالتزام من طرف جميع الدول المكونة للمجتمع الدولي ، وقد تبلور هذا الاهتمام بصـــدور الإعلان العالمي لحقوق الإنســـان الصـــادر عن الأمم المتحدة ، كما تضاعف حرص المنظمات الدولية للحفاظ على هذه الحقوق بدرجة كبيرة ، من بينها الحق في الحياة الخاصـــة للأفراد، ومن أبرز هذه الاتفاقيات أيضـــا الاتفاقية الأوروبية لحقوق الإنســـان،والاتفاقية الأمريكية لحقوق الإنســـان، والعديد من المؤتمرات الدولية في هذا الإطار، وجميعها تؤكد على حماية حقوق المواطن وحماية الحياة الخاصة للأفراد بصورتها التقليدية، لكنها حســـب وجهات النظر المختلفة لم تعالج مســـألة حماية الحياة الخاصـــة في ظل نشـــأة وتطور التكنولوجيا المعلوماتية[93].

وفي هذا الفصل ومن خلال المبحث الأول سيتم بيان معالم الحماية التي رسمتها القواعد الدولية في ظل الاتفاقيات والمؤتمرات الدولية لحماية هذا الحق ، وفي المبحث الثاني التطرق إلى واقع البيانات الشـخصـية والخصـوصـية الرقمية في فلسـطين وواقع تطبيقها وحمايتها في ظل المعايير والاتفاقيات الدولية .

[93] بارق منتظر اللامي، مرجع سابق ، ص 75

## المبحث الأول: حماية الحق في الخصـوصـية الرقمية في ظل الاتفاقيات الدولية وفي ضوء المعايير الدولية

كفلت الإعلانات والمواثيق الدولية العالمية والإقليمية حماية الحق في الخصـوصـية الرقمية بكافة أشكالها ، وجعلتها حق من حقوق الإنسان الأساسية ، التي لا يجوز تقييدها إلا بالأحوال التي بينها القانون، مما اسـتدعى بذل الجهود على المسـتوى الدولي والإقليمي لإرسـاء آليات الحماية ضـد انتهاك الحق في الخصوصية في العصر الرقمي ، وهذا ما سيتم تناوله في هذا المبحث فيما يتعلق بدور المواثيق والمعاهدات الدولية في تكريس الحق في الخصوصية الرقمية.

### المطلب الأول : الحماية الدولية للحق في الخصوصية الرقمية في المواثيق الدولية والأقليمية

تعتبر الحماية الدولية لحقوق الإنسـان ذات أهمية كبيرة نظراً للدور الذي تقوم به مختلف المواثيق والمؤتمرات الدولية في ترسيخ تلك الحقوق ودعمها في ظل النظام القانوني للدول ، ويمكن تعريف الحماية الدولية بأنها : " مجموعة الإجراءات التي يمكن أن تمارسـها الأجهزة المتخصـصـة في الأمم المتحدة أو ما تقوم به أجهزة الحماية الخاصـة المسـؤولة عن مراقبة تنفيذ الدول لالتزاماتها باحترام حقوق الإنسـان ، والتي أنشـئت بموجب اتفاقيات منشـئة للمنظمات الدولية ، أو الاتفاقيات التي تلت ميثاق الأمم المتحدة " [94]، حيث أن الحماية الدولية يجب أن تكون قد أوجبت بموجب ميثاق الأمم المتحدة، وعليه تكون هذه الحماية بموجب الميثاق حماية عامة ، فالحماية الدولية لحق الخصوصية نصت عليه مجمل المواثيق والاتفاقيات الدولية ، وقد تكاثفت الجهود الدولية والإقليمية لوضـع الإطار القانوني لحماية هذا الحق الذي يسعى لحفظ خصـوصـية الأفراد من أي انتهاك، وقد كان للإعلان العالمي لحقوق الإنسـان عام 1948 ، أثرٌ كبير في لفت أنظار العالم والشـعوب لضـرورة احترام حقوق الإنسـان وحرياته الأسـاسـية وحقه في الحياة الخاصـة ، إذ كفل الإعلان العالمي لحقوق الإنسان حق الإنسان من أي تدخل بشكل تعسفي أو غير قانوني في خصـوصـياته الشخصية .

#### الفرع الأول : الحماية المكرسة للحق في الخصوصية الرقمية في ظل المواثيق الدولية والإقليمية

أكدت لجنة الأمم المتحدة المعنية بحقوق الإنسان( مجلس حقوق الإنسان) المنوط بها قانونا تفسير مواد العهد الدولي لحقوق الإنسـان ، ومراقبة تطبيقه ، و التقيد بما جاء في المادة 17 من العهد

[94] تقرير المفوض السامي لحقوق الإنسان للأمم المتحدة حول الحق في الخصوصية في العصر الرقمي ، 2018، الملحق رقم A/HRC /39/29، ص 3.

الدولي الخاص بالحقوق المدنية والسياسية ، إذ يمثل نص هذه المادة من العهد الدولي أهم حكم تعاقدي ملزم قانوناً على الصعيد العالمي بشأن الحق في الخصوصية، حيث صادقت الغالبية العظمى من الدول الأعضاء في الأمم المتحدة على العهد ، مما يعني التزامها القانوني في إنفاذ أحكامه كافة ، بما في ذلك نص المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية ، وذلك باتخاذ تدابير تشريعية وقضائية تكفل نفاذ القانون .[95]

كما اتخذت الجمعية العامة للأمم المتحدة قرارات عدة في مجال الحقوق الرقمية ، خاصة في مجال الخصوصية وحماية البيانات، من أبرزها القرار رقم 167/68 الذي اعتمدته بتاريخ 18 ديسمبر 2013، دون تصويت وقد اشتركت في تقديمه 57 دولة من الأعضاء، بشأن الحق في الخصوصية في العصر الرقمي ، وتم التأكيد فيه أن الحقوق نفسها التي يتمتع بها الأشخاص خارج الانترنت يجب أن تحظى بالحماية على شبكة الانترنت بما في ذلك الحق في الخصوصية، وأهابت بجميع الدول أن تحترم هذا الحق وتحميه في المجال الرقمي ، وأهابت كذلك بجميع الدول أن تستعرض إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراضها وجمع البيانات الشخصية، فقد شددت على أن مراقبة الاتصالات و\ أو اعتراضها على نحو غير قانوني أو تعسفي ، وجمع البيانات الشخصية بشكل غير قانوني أمور تنتهك الخصوصية والحق في حرية التعبير، وقد تتعارض مع مبادئ المجتمع الديمقراطي، مشددة على حاجة الدول إلى ضمان تنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان تنفيذاً كاملاً وفعالاً.[96]

وقد تم استحداث **النظام الأوروبي أو القانون الأوروبي لحماية البيانات والذي دخل حيز التنفيذ في 25 مايو 2018** : ويتضمن هذا القانون أمن وخصوصية قانون أمن وخصوصية البيانات في أوروبا ، ويعتمد بشكل أساسي على الاتفاقية الأوروبية لحقوق الإنسان لعام 1950 والتي تنص على : " لكل فرد الحق في احترام حياته الخاصة والعائلية ومنزله ومراسلاته " ، إذ كرس هذا القانون إطاراً إيجابيا لحماية المستخدمين والأفراد، ويعد هذا القانون الأكثر شمولا، وقد أصبح مصدر إلهام للكثير من الحكومات والجهات التشريعية والقانونية.

ويشدد القانون الأوروبي لحماية البيانات على أن أحد المحاور الأساسية للخصوصية وحماية البيانات بعد تقييد عملية جمع البيانات هو مرحلة معالجة البيانات، حيث عرفها على أنها أي معالجة أو عملية تنفذ على المعلومات الشخصية ، سواء كانت مؤتمتة برامج وخوارزميات أو

---

95 سيفان باكرود ميسروب، حماية الحق في سرية المكالمات الهاتفية والالكترونية، مجلة بحوث مستقبلية، جامعة كركوك ، العراق،2017،ص30.

96 انظر التقرير السنوي للمفوضية السامية للأمم المتحدة لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي،2014، ص 4.

يدوية، وهو ما يشمل عملية (جمع ، تحليل ، تسجيل، تنظيم، تقسيم، تصنيف، استخدام، مسح) لبيانات المستخدمين الرقمية، الذين قد يكونوا عملاء أو مستخدمين ، أو زواراً للموقع الالكتروني ، بالإضافةِ إلى ضرورة معرفة من الشخص الذي يحق له الاطلاع على البيانات ومعالجتها، وتحديد صلاحياته بشكل واضح ومعلوم وإن كان موظفاً أو مالكاً لبيانات المستخدمين أو طرفا ثالثاً يدير هذه البيانات بشكل قانوني وآمن.[97]

كما ونصَ القانون الأوروبي لحماية البيانات على سبعة مبادئ لحماية البيانات الشخصية وتمكين المساءلة حولها، وهي على النحو التالي:[98]

1- التعامل مع البيانات الشخصية بصورة قانونية، شرعية، شفافة وعادلة ، تجاه صاحب البيانات.

2- تحديد الغرض المباشر والدقيق من معالجة البيانات ، وإعلام صاحب البيانات بها عند جمعها.

3- تقليل حجم البيانات ، التي تجمع واقتصارها على المعلومات الضرورية للغرض المحدد.

4- الحفاظ على دقة البيانات الشخصية وتحديثها ، بحيث لاتكون مغلوطة أو مضللة.

5- وضع قيود واضحة وصارمة ، على تخزين البيانات الشخصية، التي يكون للضرورة المحددة بعرض.

6- الالتزام بالنزاهة والسرية التامة في معالجة البيانات ، بما يضمن الأمان والسلامة كالتشفير.

7- مساءلة مراقب البيانات، المؤول عن جمع وحفظ ومعالجة البيانات أمام القانون.

ويعتبر هذا القانون من أصعب قوانين الخصوصية والأمن الرقمي في العالم ، كما ويفرض هذا القانون على أي فرد ينتهك معايير الخصوصية والأمان ، وذلك بعقوبات تصل إلى عشرين مليون يورو.

كما تلعب الاتفاقيات الدولية دوراً هاماً في مسألة التنسيق بين مختلف تشريعات الدول ، ومن أبرز صور التعاون الدولي في مجال حماية حق الخصوصية في المجال الرقمي :

- **الاتفاقية الامريكية لحقوق الإنسان عام 1969** : والتي دخلت حيز التنفيذ في 1987/7/18 إذ أكدت على أن : " 1- لايجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته ...2- لكل فرد أن يحميه من ذلك التدخل أو تلك الاعتداءات".[99]

---

[97] عمر أبو عرقوب، واقع الخصوصية وحماية البيانات الرقمية في فلسطين ، المركز العربي لتطوير الإعلام الاجتماعي، "حملة"،2021، ص 19

[98] هيومن رايتس ووتش،، على فلسطين إصلاح قانون الجرائم الالكترونية التقييدي،2017

[99] الفقرة 1 ، 2 من المادة 11 من الاتفاقية الأمريكية لحقوق الأنسان لسنة 1969.

**- اتفاقية بودابست المتعلقة بالإجرام المعلوماتي :**

اتفاقية بودابســـت المتعلقة بالجريمة الإلكترونية و التي دخلت حيز التنفيذ عام 2004، فقد أبرمت مجموعة من الدول الأوروبية في 23 تشـــرين الأول لســـنة 2001، اتفاقية بودابســـت للجريمة السيبرانية ، تعد هذه الاتفاقية من أهم الاتفاقيات التي كافحت الجرائم المعلوماتية المتعلقة باستخدام الانترنت وكل جرائم الحاسب الآلي، ونصت الاتفاقية على الشروط الواجب توافرها لقيام الجريمة المعلوماتية باعتبارها تنطوي على تهديد لسرية وسلامة النظم والبيانات للأفراد ، وقد نصت المادة (2) من الباب الثاني بالاتفاقية على جريمة الاعتراض القانوني باسـتخدام الوسـائل الفنية للبيانات المتداولة الكترونياً بين الحواسيب عبر شبكة الانترنت ، وبموجبه تسمح بملاحقة مرتكبي الجرائم المعلوماتية ، إذ حددت الاتفاقية أيضاً المخاطر الناتجة من الجرائم المرتكبة على شبكة الانترنت ، وإيجاد الوسائل التقنية لإثباتها وضرورة التعاون للحد من مخاطرها لضمان احترام حقوق الإنسان وخصوصياته.[100]

و هذه الوثيقة تعتبر وثيقة دولية مرجعية في بناء التشـــريعات المحلية، فقد صـــنفت الجرائم الإلكترونية ضمن أربعة أصناف: 1. الجرائم المرتبطة بسرية وسلامة بيانات الكمبيوتر وأنظمته: كالدخول غير المشـــروع على نظام كمبيوتر من خلال القرصـــنة وخداع نظام حماية كلمة الســـر واسـتغلال ثغرات البرمجيات؛ والاعتراض غير المشـروع للبيانات كانتهاك خصـوصـية إرسـال البيانات؛ والتدخل في البيانات من خلال الشـفرات الخبيثة والفيروسـات؛ والتدخل في الأنظمة بما يعوق الاسـتخدام المشـروع لها؛ وإسـاءة اسـتخدام الأجهزة وهي الأدوات المسـتخدمة في الجرائم الإلكترونية 2. الجرائم المرتبطة بالحاسوب : وهي الجرائم المتعلقة بالتزوير والاحتيال والسرقات الإلكترونية 3. الجرائم المرتبطة بالمحتوى: اســـتغلال الأطفال في إنتاج مواد إباحية 4. الجرائم المرتبطة بانتهاك حقوق الملكية الفكرية،[101] وقد جاءت المواد العقابية الواردة في اتفاقية بودابسـت ضمن (13) مادة موضوعية

ونستنتج أن هذه الاتفاقية أضفت بصورة واضحة وصريحة حماية لحق الخصوصية على شبكة الانترنت ، وأن أي انتهاك لهذا الحق يعد انتهاكاً لأحكام الاتفاقية ، وعلى الدول أن تَفعِل هذه الاتفاقية لأهميتها ، ولأنها توفر ضـمانة كبيرة لحماية خصـوصـية الأفراد وحصـانة من اختراق خصـوصـياتهم على شـبكة الانترنت ومواقع التواصـل الاجتماعي، كما شـكلت هذه الاتفاقية خطوة

[100] سيفان باكرد ميسورب، المرجع السابق ، ص35

[101] التقرير التفسيري لاتفاقية بوادبست لمكافحة الجريمة الالكترونية ، مجلس أوروبا لحقوق الإنسان، www.rm.coe.int

رائدة للتعاون بين الدول في مكافحة الجريمة الالكترونية، وترتكز أهمية هذه الاتفاقية بفعالية إقرارها للإجراءات العملية ، والتزام الدول بإدراجها في قوانينها الوطنية .

- **الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات :** تبنت جامعة الدول العربية أول اتفاقية عربية لمكافحة جرائم تقنية المعلومات في سنة 2010، وسارت هذه الاتفاقية على نهج الاتفاقية العالمية بوادبست من خلال الإقرار بالتزام الأطراف بتجريم شتى أساليب الاعتداء على حقوق الأفراد في المجال الالكتروني، والمنصوص عليه في الفصل الثاني بالاتفاقية تحت عنوان التجريم ، وركزت فيه على الدخول غير المشروع والاعتراض غير القانوني للبيانات الشخصية ، والاعتداء على سلامة البيانات ، والنص بشكل مباشر في المادة 14 منها على تجريم الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات.

كما ونجد أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أضافت على اتفاقية بودابست في الجرائم المرتبطة بالمحتوى الجرائم التالية: الجرائم المرتبطة بالمواد الإباحية عموماً وليس فقط المرتبطة باستغلال الاطفال في الأعمال الإباحية، والجرائم المتعلقة بالإرهاب المرتكبة بواسطة تقنية المعلومات، والجرائم المتعلقة بغسل الأموال والترويج للمخدرات والاتجار بالأشخاص والاتجار بالأعضاء البشرية والاتجار غير المشروع بالأسلحة، من ثم توسعت في المادة (21) لتشمل جميع الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات، هذا مع الإشارة إلى أن المواد العقابية في الاتفاقية العربية جاءت ضمن (21) مادة.

أما الميثاق العربي لحقوق الإنسان الصادر في سنة 2004 فقد جاء فيه في المادة 21: "لايجوز تعريض أي شخص على نحو تعسفي أو غير قانوني للتدخل في خصوصياته أو شؤوون أسرته أو مراسلاته أو التشهير بما يمس شرفه".[102]

جدير بالذكر أن الميثاق العربي لحقوق الإنسان بموجب التشريعات الداخلية العربية قد قيَد ممارسة الكثير من الحقوق والحريات الواردة فيه.

وعلى صعيد المؤتمرات الدولية فقد ظلت فكرة حماية الخصوصية الرقمية وحماية الحريات من التهديد التكنولوجي باستخدام الوسائل المتعددة كالتنصت والتسجيل موضوع يستحق الاهتمام من قبل العديد من الدول، فعقدت مؤتمرات دولية تحت مظلة الأمم المتحدة تتعلق بحماية الحياة الخاصة وحرمتها ومن أبرزها :

[102] المادة 21 من الميثاق العربي لحقوق الإنسان لسنة 2004.

- **المؤتمر الدولي الخامس للقضاء في فلورنسا 1976 :**

حيث ناقش دور القضـــاء في توفير الحماية القانونية اللازمة لحرية المراســـلات وســـريتها والمكالمات الهاتفية في مواجهة التطور التكنولوجي للمعلومات ، وقد ذهب المؤتمر إلى القول : " إن التقاط المكالمات الهاتفية والقيام بأخذ صـور مفاجئة وبشـكل سـري لايؤذن إلا في الحالات التي يحددها القانون وبعد استحصال الإذن من القضاء في ممارستها ."[103]

- **المؤتمر الدولي لحقوق الإنسان والذي عقد في طهران سنة 1968 :**

فقد أبدى المؤتمرون اهتماما واضـــحاً بحرمة الحياة الخاصـــة في مواجهة التطور التكنولوجي للمعلومـات، إذ أكـد في البنـد 18 منـه ؛ أن الحـدث عن المكتشـــفـات العلميـة وخطوات التقدم التكنولوجي رغم كونه فتح آفاقا واسـعة للتقدم الاقتصـادي والاجتماعي والثقافي ، يمكن أن يعرض حريات الأفراد وحقوقهم للخطر وبالتالي جعله محل البناء المتواصل .[104]

هذا و إن أغلب الدســاتير الوطنية والوثائق الدولية لحقوق الإنســان تحتوي في الغالب على إقرار للحق في الخصــوصــية، وعلى إقرار في الحق إلى الوصــول إلى المعلومة بنصــوص واضــحة وصريحة أو بنصوص ضمنية تقرر هذين الحقين للأفراد في ممارسة الحقوق والحريات.

كما يتمتع المواطن الرقمي بحزمة من الحقوق مثل الخصـوصـية وحرية التعبير كما أسـلفنا سـابقاً، وذلك إلى جانب واجب الدولة بسـن التشـريعات ووضـع القوانين لمواطنيها في دسـتورها، فإن هذه الحقوق والمســؤوليات تتطلب أن تكون في بيئة تكامل وليس تعارض، ولابد من التوعية للمواطن الرقمي بحيث يتعرف على الاستخدام اللائق للتكنولوجيا حتى يصبح منتجاً وفعالاً، وأن تقوم الدول والمجتمعات بســن القوانين لتنظيم البيئة الرقمية ومعالجة الإشــكالات التي تنتج عن الاســتخدام الخاطئ والممارســات الســلبية،وهذه القوانين تعالج مســألة الأخلاقيات الرقمية، لفضــح ومعاقبة الاســتخدام غير الأخلاقي للتكنولوجيا أو ما يســمى الجرائم الرقمية أو الألكترونية لحماية حقوق الأفراد وتحقيق الأمن والأمان له رقمياً، حيث توجد قوانين عدة ســنها المجتمع الرقمي لا بد من الانتباه لها، وكل مخالف يقع تحن طائلة هذه القوانين، مثل اختراق معلومات الآخرين أو ســرقة بياناتهم أو نشر الفيروسات وغير ذلك من الجرائم.[105]

---

[103] رافع خضرصالح، الحق في الحياة الخاصة وضماناته في مواجهة استخدامات الكمبيوتر، رسالة ماجستير ، جامعة بغداد ، العراق ،1993، ص204.

[104] رافع خضر صالح ، المرجع السابق ، ص 156.

[105] مأمون مطر، نادر صالحة، تحديات الحقوق الرقمية في فلسطين، المركز الفلسطيني للتنمية الحريات الإعلامية " مدى"،2020، ص 11

بالرغم من وجود العديد من الاتفاقيات والمعاهدات والمؤتمرات الدولية لحماية الخصـــوصـــية الرقمية، إلا أن هناك العديد من التحديات التي تواجهها ، ومع التطورات المتلاحقة في مجال التكنولوجيا فإنها تحتاج لأطر قانونية وتنظيمية جديدة لحماية الحق بشكل فعال .

**الفرع الثاني : قرارات وتوصيات الأمم المتحدة وأجهزتها بشأن حماية الحق في الخصوصية الرقمية**

يوفر القانون الدولي لحقوق الإنسان الإطار العالمي الذي يجب أن يقيَم على ضوئه أي تدخلات في الخصوصية الفردية ، وكما ورد في نص المادة 12 من الإعلان العالمي لحقوق الإنسان على أنه: " لا يعرَض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته ، أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات" ووفقاَ للمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية، والتي صادقت عليه 167 دولة ، بأن لا يجوز تعرض أي أحد بشكل تعسفي للتدخل في خصوصياته أو تعرضه لأي حملات غير قانونية تمس شرفه أو سمعته كما ذكرنا سابقاَ، وتشير هذه المادة أيضا إلى أن من حق كل شخص أن يحميه القانون من التدخل أو المساس بخصوصياته.

كما وتتضمن صكوك دولية أخرى لحقوق الإنسان أحكاماً مماثلة، إضافةً إلى ذلك تعكس القوانين على الصـــعيدين الإقليمي والوطني أيضـــاً حق جميع الأشـــخاص في أن تُحترم حياتهم الخاصـــة وحياتهم العائلية وسكنهم ومراسلاتهم أو الحق في الاعتراف بكرامتهم أو سلامتهم الشخصية أو سمعتهم واحترامها ، وبعبارة أخرى، هناك اعتراف عالمي بالأهمية الأساسية والصلة الوطيدة للحق في الخصوصية والحاجة إلى ضمان حماية هذا الحق في القانون والممارسة. [106]

وقد قدمت كل من هيئات المعاهدات الدولية والإقليمية لحقوق الإنســـان والمحاكم والمؤتمرات واللجان والخبراء ، إرشـــادات فيما يخص نطاق ومحتوى الحق في الخصـــوصـــية ، ومن أهم القرارات التي أقرت بأهمية حماية الحق في الخصوصية في العصر الرقمي :

- **قرار الجمعية العامة للأمم المتحدة الخاص بالحق في الخصوصية في العصر الرقمي المؤرخ في 2013/12/18 :** فقد صدر تقرير الحق في الخصوصية في العصر الرقمي من قبل المفوض السامي لمجلس حقوق الإنسان بغرض حماية وتعزيز الحق في الخصوصية في ضوء التطور التكنولوجي وزيادة قدرة الدولة على مراقبة الأفراد، حيث قدم التقرير مجموعة من النتائج التي

[106] المرجع السابق، التقرير السنوي للمفوضية السامية للأمم المتحدة لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي،2014، ص 6.

انبثقت عن عاملين رئيسيين في مجال الخصوصية الرقمية وهما : استقراء الممارسات في هذا المجال بالنظر إلى أنها المصدر الأول لتشكيل القانون الدولي ، أما العامل الثاني فيكمن في إحداث توازن بين هذه الممارسات والموقف التقليدي لقواعد القانون بشان الحق في الخصوصية.[107]

**- قرار مجلس حقوق الإنسان بحماية حقوق الإنسان على الانترنت والمؤرخ في 2016/7/1:**

إذ أكد القرار على أن حقوق الإنسان التي يتمتع بها الأفراد خارج شبكة الانترنت يجب حمايتها عبر الانترنت ، وأن شبكة الانترنت يمكن أن تكون أداة مهمة لممارسة وتطبيق حقوق الإنسان، ودعا القرار إلى احترام وحماية حقوق الإنسان على الانترنت ، وإلى تعزيز وتسهيل وصول الأفراد إلى الانترنت والاستثمار في محو الأمية الرقمية، واحترام الحق في حرية التعبير على شبكة الانترنت ، ومكافحة خطاب العنف والكراهية وذلك حسبما ورد في الفقرة الثامنة من هذه القرار.[108]

**- التعليقات العامة للجنة المعنية بحقوق الإنسان حول الحق في الخصوصية الرقمية:**

شددت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم 16 ، على أن الامتثال للمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية يقتضي ضمان سلامة المراسلات وسريتها بحكم القانون وبحكم الواقع، وينبغي أن تقدم المراسلات إلى الجهة المرسل إليها دون أن يعترضها أحد ودون أن يفتحها أو يقرأها بطريقة أخرى .[109]

القانون الدولي لحقوق الإنسان لا يجيز التدخل في حق الأفراد في الخصوصية، إلا إذا لم يكن هذا التدخل تعسفياً ولا غير قانوني، وقد أوضحت اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم 16 أيضاً ، أن مصطلح " غير قانوني" يعني عدم إمكانية حدوث أي تدخل " إلا في الحالات التي ينص عليها القانون، ولايجوز أن يحدث التدخل الذي تأذن به الدول إلا على القانون الذي يجب أن يكون هو نفسه متفقاً مع أحكام العهد الدولي وأهدافه، أي أنه وبعبارة أخرى فإن التدخل المسموح به بموجب القانون الوطني قد يكون " غير قانوني" ، إذا كان القانون الوطني يتضارب مع أحكام العهد الدولي الخاص بالحقوق المدنية والسياسية ، وعليه من الممكن أن تتسع عبارة "التدخل التعسفي " لتشمل التدخل المنصوص عليه بموجب القانون، وأوضحت اللجنة أن " المقصود بإدراج مفهوم التعسف هو ضمان أن يكون التدخل نفسه الذي يسمح به القانون موافقاً لأحكام العهد الدولي للحقوق المدنية والسياسية وأهدافه، وأن يكون في جميع الحالات معقولاً بالنسبة للظروف

---

[107] د.رزق سمودي وآخرون ،الموقف المعاصر للقانون الدولي العام من الحق في الخصوصية في العصر الرقمي ، مجلة الجامعة العربية الأمريكية للبحوث، مجلد 3،العدد 2، فلسطين، 2017، ص 11

[108] ينظر قرار رقم A/HRC/RES/ 32/13 مجلس حقوق الإنسان اعتمد في 2016

[109] *الوثائق الرسمية للجمعية العامة، الدورة الثالثة والأربعون، الملحق رقم 40* (A/43/40)، المرفق السادس، الفقرة 8.

المعنية التي يحدث بها فيها ، كما فسرت اللجنة المعنية على أن " أي تدخل في الخصوصية يجب أن يتناسب مع الغرض المنشود ، ويجب أن يكون ضرورياً في أي مسألة معينة".[110]
وتنص اللجنة المعنية بحقوق الإنسان في تعليقها العام رقم 31 بشأن طبيعة الالتزام القانوني الذي يقع على عاتق الدول الأطراف في العهد ، على أن الدول الأطراف يجب أن تُحجم عن انتهاك الحقوق المعترف بها في العهد ، وأن " أية قيود تفرض على تلك الحقوق يجب أن تكون مباحة بموجب الأحكام ذات الصلة من العهد ، وعلى الدول عند فرضها أية قيود ، أن تقيم الدليل على ضرورتها والاّ تتخذ من التدابير إلا ما يكون متناسبا مع تحقيق الأهداف المشروعة بغاية ضمان الحقوق المنصوص عليها في العهد الدولي للحقوق المدنية والساسية حماية مستمرة وفعالة".[111]

**الفرع الثالث : مبادئ حماية الخصوصية الرقمية والبيانات الشخصية وفقاً للمعايير الدولية**

تشكل المبادئ التي تستند إليها الخصوصية الرقمية وحماية البيانات جزءاً رئيسياً من النظم القانونية ذات الصلة وهي في صميم أطر حماية البيانات، إذ أنها تؤدي وظيفة مزدوجة، من حيث تفسير وإدماج الإطار التنظيمي، وذلك من أكثر الوسائل وضوحاً ومنتجاً لمعالجي البيانات والمتحكمين بها الذين يقومون بالمعالجة الصحيحة للمعلومات والبيانات الشخصية لا سيما عند مواجهة انتهاكات وسائل استخدام وسائل التكنولوجيا والاتصالات ، كما تسعى هذه البيانات إلى إيجاد حماية فعالة لحقوق المستخدمين وتطويرها، ووضع الأساس القانوني لمعالجة البيانات ، وتدابير الأمن وآليات الرقابة، وفي هذا الفرع سيتم تحليل هذه المبادئ ، إذ تشكل هذ أسس النظام القانوني والتدخل المشروع في حماية الخصوصية الرقمية والبيانات الشخصية، وتعتبر أيضاً "معايير دنيا" لحماية الحقوق الأساسية للبلدان التي صادقت على الاتفاقيات الدولية لحماية البيانات، هي تشكل معياراً للحكم على إجراءات الدول في ما يتعلق بمدى احترامها وحمايتها للحق في الخصوصية، وهذه المبادئ ملزمة للدول من الناحية القانونية بالاستناد إلى الالتزام التعاهدي على الصعيد الدولي والإقليمي ، كذلك فإن هذه المبادئ تستجيب للتطورات التكنولوجية التي طرأت على تكنولوجيا المعلومات، كما يجب أن تكون أساس أي قانون لحماية البيانات ، وقد وردت هذه المبادئ في القرارات الصادرة عن الأمم المتحدة، لاسيما المقرر الخاص المعني بالحق في الخصوصية ، والمقرر الخاص المعني بحرية الرأي والتعبير، كما وردت هذه المبادئ في آراء

110 المرجع السابق التقرير السنوي للمفوضية السامية للأمم المتحدة لحقوق الإنسان ،ص 9.
111 انظر التعليق العام رقم 31 (80) ،اللجنة المعنية بحقوق الإنسان، الدورة الثامنة عشرة ،العهد الدولي الخاص بالحقوق المدنية والسياسية ، الفقرة 6 CCPR/C/21/Rev.1/Add. 2004

خبراء مختصـين في الخصـوصـية والأمن الرقمي، ووردت أيضـا في القانون الأوروبي لحماية البيانات ، ومعظم قوانين حماية البيانات المعمول بها في أمريكا اللاتينية ، و ، وهذه المبادئ هي :[112]

- **مبدأ القانونية والشرعية :** ويشير هذا المبدأ إلى أن أي تدخل بالخصوصية يجب أن يكون قد نص عليه القانون الصادر عن السلطة المختصة في الدولة ، وأن يكون القانون واضحاً ودقيقاً بما يكفي ومعلوماً للكافة ، بحيث يمكن لأي فرد أن ينظر إلى القانون، ويتأكد ممن يؤذن له القيام بمراقبة البيانات وفي أي ظروف ولضمان علم الأفراد المسبق به حتى يتجنبوا تعسف السلطات في استخدامه ، كما يجب أن يحدد القانون الجهة المختصة بالإذن بالتدخل وإجراءات التدخل ، وهدفه ومدته، وغيرها من الأحكام التنظيمية التي يترتب على عدم تطبيقها ، عدم مشروعية التدخل ، كما وتستند قانونية معالجة البيانات الشخصية إلى وجود أسباب مشروعة منصوص عليها في اللوائح التنظيمية المعمول بها

- **مبدأ المشروعية :** بمعنى أنه يجب أن يكون التقييد ضرورياً للتوصل إلى هدف مشروع، كما يجب أن يكون متناسباً مع الهدف وأن يكون أقل الخيارات اقتحاماً للحياة الخاصة ، وعلاوة على ذلك، يجب بيان أن التقييد المفروض على الحق (تدخل في الخصوصية، مثلاً، لأغراض حماية الأمن القومي أو حق الآخرين في الحياة) يحتمل أن يحقق ذلك الهدف، وهنا يقع عبء إثبات أن للقيد علاقة بهدف مشروع على عاتق السلطات التي تسعى إلى تقييد الحق، وعدم تعارضه مع ما هو مقبول في المجتمعات الديموقراطية.

**-مبدأ الضرورة والتناسب:** بمعنى ألَا يجرد أي تقييد للحق في الخصوصية جوهر الحق من معناه ، وأن يكون ضرورياً لتحقيق غرض قانوني مشروع ، و يكون متسقاً مع حقوق الإنسان الأخرى، ويقع على الدولة أيضاً عبء إثبات هذه المبرر، وفي هذا السياق تقول اللجنة المعنية لحقوق الإنسان :"لا يكفي أن تخدم القيود الأغراض المسموح بها ، فيجب ان تكون ضرورية لحمايتها " وأوضحت كذلك أن التدخل يجب أن يكون أقل الوسائل تدخلاً مقارنة بغيره من الوسائل التي يمكن أن تحقق النتيجة المنشودة ، وعندما لا يستوفي التقييد هذه المعايير، سيكون التقييد غير قانوني و/أو يكون التدخل في الحق في الخصوصية تعسفياً، كما يجب أن يؤخذ بعين الاعتبار نطاق التدخل وحساسية المعلومات المتحصل عليها ، ويكون التدخل متناسبا إذا كان مقتصراً فقط على خدمة الغرض القانوني المشروع الذي تم على أساسه الإذن بالتدخل وأي معلومات أخرى لا تخدم

[112] انظر مبادئ سيراكوزا المتعلقة بأحكام التقييد وعدم التقيد الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية، الفقرة 33 ، https://docstore.ohchr.org

الغرض المعين وتم الحصـــول عليها من التدخل المأذون به ســـوف لن يتم التعويل عليها أو اسـتخدامها حتى وإن كانت تخدم غرض مشـروع آخر، كما يجب ووفقاً لهذا المبدأ عدم الاحتفاظ بالمعلومات المتحصـــل عليها بعد اســـتخدامها في الغرض الذي لأجله تم الحصـــول عليها ، وذلك بإتلافها أو إعادتها إلى أصحابها. [113]

- **مبدأ الموافقة:** وهذا المبدأ مرتبط ارتباطاً وثيقاً بمبدأ القانونية، ووفقاً لهذا المبدأ يجب أن يشـــير أصحاب البيانات إلى أنهم يقبلون يجمع بياناتهم الشخصية وتسجيلها ومعالجتها أو نقلها ، أو تخضع لأي نشـــاط معالجة أو حتى للحذف ، وهي مظهر من مظاهر الإرادة الصـــريحة أوالضـــمنية التي تلزم الشخص الموافق قانوناً ، كما يتربط هذا المبدأ بمبدأ الشفافية ، إذ أن الموافقة من قبل صاحب البيانات تعني أن يبلغ صـاحب هذه البيانات [114]على النحو الملائم بالظروفالتي ستخضـع لها بياناته الشخصية.

- **مبدأ الشـــفافية**: وتعني أن يتم معالجة البيانات بطريقة شـفافة من قبل المتحكمين بالبيانات ، وأن يتم إبلاغ أصـحاب البيانات بظروف المعالجة التي ستخضـع لها بياناتهم ، كما ويشـترط الإفصـاح عن الأساس القانوني الذي يجيز معالجة البيانات.

- **تحديد الغرض** : ويتم ذلك بأن لا يتم جمع البياناتالشخصية ومعالجتها إلا لغرض محدد وصـريح وأن لا يتجاوز مدة زمنية محددة ، وأن لا تتم المعالجة بأي طريقة لا تتفق مع هذا الغرض.

- **تحديد المدة للاحتفاظ بالبيانات:** لا يجوز الاحتفاظ بالبيانات والمعطيات شـخصـية لمدة طويلة أو مما هو مطلوب.

- **تقليص البيانات** : بأن يقتصـــر جمع البيانات الشـــخصـــية واســـتخدامها على غرض محدد ويفي بالغرض التي جمعت من أجله .

- **الإنصاف**: ويقصد بهذا المبدأ أن لا يتم التعامل مع هذه البيانات أو معالجتها أو استخدامها لغايات تتعارض مع المبادئ المنصـوص عليها في ميثاق الأمم المتحدة، وأن لا يمارس ضـد صـاحب هذه المعطيات والبيانات أي أشـكال من التمييز التعسـفي، وتنفذ معالجة البيانات وفقاً للمبادئ والمعايير الدولية.

[113] CCPR/C/21/Rev.1/Add.9 ، الفقرات 11- 16

- **مبدأ جودة البيانات ودقتها**: بمعنى أن تكون البيانات الشخصية دقيقة وصحية وكاملة ، وقابلة للتحديث عند الضرورة وذلك من قبل المتحكم بالبيانات أومعالج البيانات أو بناء على طلب صاحبها ، ويكون القدرة للمتحكمين بها القدرة على معرفة أن هذه البيانات تستوفي المواصفات.

-**مبدأ الأمن وحقوق المستخدمين** : بحيث تتم المعالجة وفقاً لحقوق المستخدمين مثل الحق في الحذف أو النفاذ إلى المعلومة ، وضمان سرية البيانات وسلامتها وتجنب أي مخاطر قد تتعرض لها كالوصول غير المصرح به، أو إتلافها. [115]

جدير بالذكر بان هذه المبادئ التوجيهية لا تعتبر توصيات ، وإنما تشكل جزءاً هيكيلياً من النظم القانونية لأهميتها، وتلزم المتحكمين بالبيانات ومعالجيها بالتصرف على النحو الملائم عند جمع البيانات وتخزينها ومعالجتها ، أو تعرضها لأي نوع من الانتهاكات.

## المطلب الثاني:آليات حماية الحق في الخصوصية الرقمية في ضوء قواعد القانون الدولي والمعايير الدولية

يوفر القانون الدولي لحقوق الإنسان على الصعيد العالمي إطاراً قانونياً لحماية الحق في الخصوصية بمفهومه العام، والجدير بالقول أن أحكام بعض هذه المواثيق والاتفاقيات قد ارتقت وأصبحت قواعد عرفية مما يعني التزام الدول بها لو كانت غير موقعة على الاتفاقيات،[116] إلا أنه ذلك وحده لا يكفي لحماية الخصوصية في العصر الرقمي ، بل كان للأمم المتحدة دوراً بارزا في حمل المجتمع الدولي على الاعتراف بها الحق، وإقرار آليات لحماية هذا الحق في ضوء قواعد القانون والاتفاقيات الدولية ، وفي هذا المطلب نلقي الضوء على مدى كفاية الأطر العالمية لحماية الحق في الخصوصية الرقمية ومدى التزام الدول باحترام الحق في الخصوصية الرقمية كحق أصيل من حقوق الإنسان وجميعها تندرج في إطار آليات حماية الحق في الخصوصية في الرقمي تحت مظلة القانون الدولي والمعايير الدولية.

### الفرع الأول : مدى كفاية المواثيق الدولية لحماية الحق في الخصوصية الرقمية

كما سبق الذكر فقد تم الاعتراف بالحق بالخصوصية لأول مرة وفقاً للمادة 12 من الإعلان العالمي لحقوق الإنسان ، وكما تناولته المادة 17 من العهد الدولي الخاص بالحقوق المدنية

---

[115] انظر المبادئ التوجيهية التي تستند إليها الخصوصية وحماية البيانات الشخصية ، تقرير الجمعية العامة للأمم المتحدة رقم A /77/196، المؤرخ 2022/7/20

[116] د.رزق سمودي،، وآخرون،الموقف المعاصر للقانون الدولي العام من الحق في الخصوصية في العصر الرقمي ، مجلة الجامعة العربية الأمريكية للبحوث، مجلد 3،العدد 2، فلسطين، 2017، ص 9

والسياسية والتي نصت على : "1-لايجوز تعرض شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته ولا لأي حملات تمس شرفه أو سمعته.2- من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس ".[117]

نظراً لانتشـار التكنولوجيا والتطور العالمي في المناطق المختلفة حول العالم ، فإنه يرى جانب من الفقه ضـرورة تعديل المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسـياسـية، وذلك لأن المبادئ التي وضعت وفقاً للعهد الدولي قبل أكثر من خمسين سنة حين صياغة العهد الدولي تحتاج إلى التطوير لجعلها أكثر ملائمة مع نتائج التطورات التكنولوجية الحديثة.

فعندما اعتمد التعليق العام رقم 16 على المادة 17 من العهد الدولي للحقوق المدنية والسياسية في العام 1988، كان التقدم التكنولوجي على الحق في الخصـوصـية ليس واضـحاً كما هو الشـأن اليوم، فلقد أدى التطور في تكنولوجيا المعلومات والاتصـالات والذي يرتبط بشـبكة الانترنت ، والاهتمام الحالي بجمع البيانات الشخصية سواء من طرف الدول أو الشركات إلى انتهاك وتقويض هذا الحق بشكل كبير مؤخراً ، لذلك كان هناك العديد من المطالبات والنداءات للجنة المعنية بحقوق الإنسان في الأمم المتحدة لصياغة تعليق جديد، أو تحديث التعليق العام رقم 16، وأن يتم من خلال التحديث توضيح ما يعنيه الحق في الخصوصية الرقمية وما هي المعلومات التي يتوجب حمايتها، إلى جانب تحديد نطاق التزامات الدول بموجب معاهدات حقوق الإنسان.[118]

وهذا ما أكد عليه قرار الجمعية العامة للأمم المتحدة رقم 73/179 الذي ينص على أنه :"ونظراً للتطور الكبير الذي حصـل منذ اعتماد التعليق العام رقم 16 ، الصـادر عن اللجنة المعنية بحقوق الإنسان على المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية ، فإن هناك حاجة إلى إعادة مناقشة مفهوم الحق في الخصوصية في العصر الرقمي ."[119]

وكانت قد تبنت اللجنة الاجتماعية والانسانية والثقافية (اللجنة الثالثة) للدورة الثامنة والستين (68) للجمعية العامة للأمم المتحدة في نيويورك في العام 2013، قراراً بالإجماع ينص على الحق في الخصـوصـية في العصـر الرقمي ، كانت قد تقدمت به في الأسـاس البرازيل وألمانيا، ثم انضـمت اليهما لاحقاً أكثر من خمسين دولة، ويأتي هذا القرار الذي أكد على حق الانسـان في الخصـوصـية وعلى عدم السـماح بتعريضـه للتدخل في خصـوصـياته، بعد الكشـف عن انتهاكات واسـعة النطاق للحق في حرمة الشـؤون الشـخصـية لمواطنين في أنحاء مختلفة من العالم، وقد اعتمدت اللجنة

---

[117] انظر العهد الدولي الخاص بالحقوق المدنية والسياسية ، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 2200(د-21) ،المؤرخ في 16 ديسمبر 1966

[118] عائشة غزيل، الحماية الدولية للحق في الخصوصية في العصر الرقمي ، جامعة غليزان، الجزائر، 2022، ص 409

[119] قرار الجمعية العامة رقم 69/173 حول الحق في الخصوصية في العصر الرقمي ، الملحق رقم A/RES/73/179

الاجتماعية والانسـانية والثقافية التابعة للجمعية العامة للأمم المتحدة نصـاً معدلاً للنص الأصـلي الذي تقدمت به البرازيل وألمانيا، ، ويتضـمن مواقف مهمة بشـأن حق الانسـان في الخصـوصـية ، حيث أنه:

يؤكد على « حق الانسان في الخصوصية الذي لا يسمح بتعريض أي شخص، على نحو تعسفي أو غير قانوني، للتدخل في خصوصياته أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخّل ،و يرحب بتقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير بشـأن تداعيات مراقبة الدول للاتصـالات على ممارسـة حق الانسـان في الخصـوصـية وفي حرية الرأي والتعبير، كما يشدد على أن مراقبة الاتصـالات واعتراضـها وجمع البيانات الشخصية على نحو غير قانوني أو تعسفي تنتهك الحق في الخصوصية والحق في حرية التعبير ، وقد تتعارض مع مبادئ المجتمع الديمقراطي، هذا ويؤكد أن الحقوق نفسها التي يتمتع بها الأشـــخاص خارج الانترنت يجب أن تحظى بالحماية أيضـــاً على الانترنت، بما في ذلك الحق في الخصـوصـية، ويهيب بالدول كافة احترام وحماية الحق في الخصـوصـية بما في ذلك في سـياق الاتصـــالات الرقمية، واتخاذ ما يلزم لوضـــع حدّ للانتهاكات لتلك الحقوق، واعادة النظر في ممارســات المراقبة، وانشــاء آليات رقابة محلية مســتقلة، كما طلب من مفوضــية الأمم المتحدة السـامية لحقوق الانسـان أن تقدم الى الدورة 27 لمجلس حقوق الانسـان والى الدورة 69 للجمعية العامة تقريراً عن حماية الحق في الخصـوصـية وتعزيزه في سـياق مراقبة الاتصـالات الرقمية، يتضمن آراء وتوصيات لكي تنظر فيه الدول الأعضاء.

وقد أضافت مجموعة كبيرة من الدول أسماءها الى جانب البرازيل وألمانيا كمقدمة لمشروع القرار المعدل الذي تم اعتماده بالإجماع، من بينها ثلاث دول عربية هي لبنان، مصر وتونس.

واعتبر مندوب ألمانيا في كلمته لمشـــروع القرار قبل اعتماده، أن الميثاق الدولي للحقوق المدنية والسـياسـية لعام 1966، يعطي رغم قدمه في بنديه 2 و17 قاعدة صـلبة للقرار الذي تم طرحه ، وأشـار الى أن عملية المتابعة الشـاملة لهذا الموضـوع مسـتمرة وسـتناقش الدول الأعضـاء بشـكل مفصل المسائل المطروحة في هذا الشأن، بينما توقع مندوب البرازيل أن يطلق صدور هذا القرار، نقطة محورية للعصر الحديث حول المراقبة واحترام حقوق الانسان في الفضاء الافتراضي.

وكان مجلس حقوق الانســان قد أصــدر في يوليو عام 2012 قراراً بشــأن تعزيز وحماية حقوق الانسـان على الانترنت، أكد فيه " أن نفس الحقوق التي يتمتع بها الأشـخاص خارج الانترنت يجب

أن تحظى بالحماية أيضـاً على الانترنت "، وقد لاقى هذا القرار الترحيب باعتباره أول قرار للأمم المتحدة يؤكد على حماية حقوق الانسان في العالم الرقمي.[120]

الفرع الثاني: التزام الدول باحترام الحق في الخصوصية الرقمية باعتبارها حق من حقوق الإنسان وفقاً لجهود الأمم المتحدة لحماية الحق في الخصـوصـية الرقمية ، فإن مسـؤولية الدول أن تحمل وتصـون هذا الحق وفقاً للالتزامات المقررة بموجب القانون الدولي لحقوق الإنسـان، ومن المعلوم بأن قرارات الأمم المتحدة بشأن الحق في الخصوصية الرقمية تمثل تطوراً كبيراً ، وقد شدَدت هذه القرارات في مجملها على التزام الدول بوضع مسألة مراقبة الاتصالات والبيانات الرقمية في إطار القانون الدولي لحقوق الإنسـان، وأن تسـتند في ذلك إلى المادة 12 من الإعلان العالمي لحقوق الإنسـان، والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسـياسـية، كما اعتمدت الجمعية العامة ومجلس حقوق الإنسان العديد من القرارات بهذا الخصوص ، وشددت كما سبق القول على اعتبار الحقوق التي يحظى بها الأشـخاص خارج الانترنت يجب ان تحظى بالحماية على شـبكة الانترنت ، وفي هذا الصـدد حث قرار الجمعية العامة رقم 67/168 الدول على احترام الحق في لخصوصية الرقمية ، وأضاف أيضا في نفس السياق قرار مجلس حقوق الإنسان رقم 32/13 أن الحقوق التي يتمتع بها الأشخاص خارج الانترنت يجب أن تحظى أيضاً بنفس الحماية على شبكة الانترنت.

بناء على ذلك فإن قرارات الأمم المتحدة في هذا الخصـوص كلها تؤكد على أن القانون الدولي ينطبق على استخدام الدول للتكنولوجيا ووسائل الاتصالات، وأن جهود الدول للتصدي وحماية أمن المعلومات والاتصـالات يجب أن تكون متلازمة مع حقوق الإنسـان والحريات الأسـاسـية المبنية على الإعلان العالمي لحقوق الإنسان والصكوك الدولية .

ومن الضـروري أن تقوم الدول بتوفير ضـمانات لحماية الخصـوصـية في العصـر الرقمي وهذه الضمانات هي :

- **الضـمانة التشـريعية**: إن قرارات الأمم المتحدة تشـدد على أن تكون التشـريعات وفق التزامات الدول بحقوق الإنسان فعالة لحماية الحق في الخصوصية، وأن تنطوى على جزاء أو عقوبة جراء المس بهذا الحق ، وهذا ما تم تناوله في قرار الجمعية العامة رقم 179/73 بضرورة اعتماد الدول تشـريعات ولوائح لحماية بياناتها، وأن تمتثل للالتزامات الدولية ، وقد نص القرار أيضـاً على أن لوائح البيانات للدول يجب أن تتضمن جزاءات فعالة ، كما أكد القرار رقم168/67 على أن يجب

[120] انظر قرار اللجنة الاجتماعية والانسانية والثقافية (اللجنة الثالثة) للدورة الثامنة والستين (68) للجمعية العامة للأمم المتحدة الجمعية العامة حول الحق في الخصوصية في العصر الرقمي ، الملحق رقم A/C.3/68/L.45/Rev.1

على الدول أن تعمل على ضـمان توافق تشـريعاتها الوطنية مع التزاماتها بموجب القانون الدولي الإنساني للحيلولة دون حدوث انتهاكات على الحق في الخصوصية الرقمية، كما أقر مجلس حقوق الإنسان في توصية صادرة عنه في عام 2021، دعت الدول إلى اعتماد وإنفاذ تشريعات خاصة لحماية البيانات بطريقة فعالة من خلال سلطات مستقلة ومحايدة لحماية الحق في الخصوصية في سياق الذكاء الاصطناعي.[121]

وبالرجوع إلى التشريعات المحلية كما تم ذكرها مسبقا في الفصل الثالث من هذه الدراسة ، نجد أن العديد من الدول قد تضـمنت في منظومتها التشـريعية قوانين متعلقة بحماية البيانات أو حماية الخصوصية الرقمية، كالتشريع المصري والتشريع الأردني ، والمشرع السوري والجزائري ، والقانون الفرنسي، وقرار مجلس الوزارء الفلسطيني.

فعلى سبيل المثال قد جاء في رد الأردن على قائمة المسائل المقرر تناولها أثناء النظر في التقرير الدوري الرابع للأردن حول تطبيق العهد الدولي الخاص بالحقوق المدنية والسياسية خلال جلسة لجنة مجلس حقوق الإنسـان في جنيف سـنة 2010 ؛ أن الأردن ملتزم بالعهد الدولي الخاص بالحقوق المدنية والسياسية وأن الاتفاقيات التي صادقت عليها هي جزء لا يتجزأ من التشريع وتسموعلى القوانين الوطنية ، ويساند ذلك الاجتهاد القضائي في قرارات محكمة التمييز الأردنية ، فالقرار 2003/818 الصادر في 3 حزيران 2003 قد جاء فيه : " تسمو المعاهدات والاتفاقيات الدولية مرتبة على القوانين المحلية ولها أولوية التطبيق عند تعارضـها معها ولا يجوز الاحتجاج بأي قانون محلي أمام الاتفاقية .." ، كذلك الأمر فإن محكمة استئناف عمان كانت قد فسخت قراراً لمحكمة بداية عمان رقم 2009/550 بتاريخ 28 أيار 2009، واسـتندت في ذلك إلى المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية ، بالإضافة إلى العديد من السوابق القضائية التي تم ترجيح المعاهدات الدولية على القوانين الدولية .[122]

- **الضمانات الرقابية**: في هذا الشأن فقد دعى قرار الجمعية العامة 167/68 سالف الذكر، الدول لأن تنشئ آليات رقابة محلية مستقلة فعالة وقادرة على ضمان المساءلة والشفافية والمساءلة بشأن مراقبة الاتصالات واعتراضها وجمع وتخزين البيانات الشخصية، كما أن قرار الجمعية العامة رقم 166/69 أشـار إلى أنه يقع على عاتق الدول أن تتيح للأفراد التي انتهكت حقوقهم

---

121 انظر تقرير المفوض السامي لحقوق الأنسان في الأمم المتحدة حول الحق في الخصوصية في العصر الرقمي ، 2021، الملحق رقم A/HRC/48/31،ص 19

122 يحيى شقير، مدى توافق قانون الحصول على المعلومات في الأردن مع المعايير الدولية – رسالة ماجستير- جامعة الشرق الأوسط، الأردن، 2012، ص 37

وخصوصياتهم نتيجة المراقبة غير القانونية سبل الانتصاف الفعالة بما يتسق مع إلتزاماتها الدولية لحقوق الإنسان.

لكن لازال يوجد عقبات كبيرة أمام إتاحة المجال لسبل انتصاف الضحايا من انتهاكات الخصوصية، كما أنه تواجه الأفراد تحديات جديدة بناء على الحسابات عبر الوسائل الالكترونية ، حيث أنه لايمكن الحصول على البيانات المدخلة أو الطعن في النتائج التي توصلت إليها حسابات الخوارزميات أو معرفة الكيفية التي تم بها استخدام هذه النتائج من أجل اتخاذ القرارات والأحكام[123]، كذلك يجب أن يكون لدى الدول إلى جانب التشريعات آليات وأجهزة مستقلة لمساءلة الدولة عن انتهاكات الحق في الخصوصية الرقمية، بحيث يكون لديها صلاحيات لمراقبة ممارسة الدولة في هذا المجال ، والتحقيق في الشكاوى الواردة من الأفراد، وإصدار العقوبات على انتهاكات الخصوصية والبيانات والاتصالات بشكل غير قانوني.

[123] تقرير المفوض السامي لحقوق الأنسان في الأمم المتحدة حول الحق في الخصوصية في العصر الرقمي ، المرجع السابق ،A/HRC/39/29، ص 5

## المبحث الثاني : مظاهر الحماية الجزائية للحق في الخصـــوصـــية الرقمية في التشريعات المقارنة

لقد زاد الوعي لدى بعض الحكومات حول مخاطر الوسائل الحديثة للاتصال على الحياة الخاصة للأشخاص، وعملت على تطويقها بإصدار مجموعة من التشريعات لحماية الخصوصية والسرية، مقرة بذلك مبدأ الســـرية الالكترونية، أما بعض الدول لازالت تدرس هذا الأمر ولم تهيئ ســـوى مشـاريع قوانين لم تجد طريقها بعد إلى حيز التطبيق، أو فضـلت الاكتفاء بنصـوص تقادمت عليها الزمن.

وفيما يلي نتطرق إلى مظاهر الحماية الاجرائية للخصـــوصـــية الرقمية في القانون، والحماية الاجرائية للخصوصية الرقمية في التشريعات المقارنة

### المطلب الأول : الحماية الإجرائية للحق في الخصوصية الرقمية ومظاهر تكريس هذه الحماية

إن القانون يمنع التعاطي مع المعلومات التي تؤدي إلى انتهاك السـرية والخصـوصـية ، كما يمنع اســـتخدام البيانات لغير الأغراض التي جمعت من أجلها ، ووما لا شـــك بأنه يمكن لمس إرادة المشـــرع في تبني قواعد أجرائية لمكافحة الجرائم المعلوماتية أو الوقاية منها ، وبين تكريس الحق في الخصـــوصـــية الرقمية ، من خلال تكريس عدة مظاهر لحماية الحق في الخصـــوصـــية عبر الفضاء الرقمي وأهمها : [124]

- منع الجمع والتخزين غير المشروع للبيانات الشخصية أي البيانات ذات الطابع الشخصي، وهي التي تتمثل في أي معلومات عن الشخص التي تكون هويته محددة أو يمكن تحديدها من خلال جمع البيانات، أو عن طريق الجمع بينها وبين أي بيانات أخرى بما في ذلك الصوت والصورة.

- الانحراف عن الغرض من معالجة البيانات آلياً وهي عملية أو مجموعة عمليات تجري على البيانات الشـــخصـــية، فعند إجراء المعالجة لهذه البيانات يجب احترام الإجراءات الواجب اتباعها أثناء هذه العملية ، واحترام الغرض الذي من أجله تم الســـماح بشـــكل قانوني معالجة البيانات الشـخصـية ، وأن لا تتعداه إلى غيره من الأغراض ، وقد جرمت عدة قوانين هذا الفعل ، وعاقبت عليه من أبرزها القانون الفرنســي ، واسـتثناءاً تجيز بعض التشـريعات المقارنة إعادة معالجة هذه البيانات لغايات علمية بشـــرط الحصـــول على موافقة المعني بالأمر أو ورثته ، وبموافقة الهيئات الرسمية .

---

[124] منى تركي الموسوي ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها ، مجلة كلية بغداد للعلوم الاقتصادية ، 2013، ص 19.

- تحديد مدة الاحتفاظ بالبيانات و عدم تجاوز ها أكثر من المدة القانونية اللازمة : بقاء البيانات الشخصية مخزنة لوقت طويل لدى الجهات التي تعالج البيانات يزيد من المخاطر التي قد تتعرض لها هذه البيانات ، لذلك قامت التشـــريعات المقارنة بإلزام الهيئات القائمة بعملية إزالة المعطيات الشـــخصـــية بمجرد انتهاء الأجل المحدد لحفظها بالتصـــريح ، أو الترخيص ، أو وفقاً للقوانين الخاصـة ، وفي حالة تحقق الغرض التي جمعت من أجله ، أو إذا لم تعد ضـرورية للمسـؤول عن المعالجة ، وكذلك الحال بالنســـبة لمزودي خدمات الانترنت ، حيث يفرض عليه القانون التزاماً يتضـــمن إزالة البيانات التي تم تخزينها ، والمتعلقة بالاتصـــالات الالكترونية والخاصـــة بهوية المتصلين وساعات الاتصال .

- التأكيد على سرية المراسلات والاتصالات وحظر الإفشاء غير المشروع للبيانات الشخصية ؛ ويقصد بالإفشاء غير المشروع :" قيام الشخص المسموح له بمعالجة وحفظ البيانات الشخصية بالســماح إلى شــخص آخر غير مرخص له بالاطَلاع عليها "، وقيام فعل الإفشـــاء المجرم قانوناً يتطلب تحديد معالم الشخص الذي تتعلق به البيانات التي تم إفشاؤها على نحو يمكن التعرف عليه، كما ويمكن أن يتم إفشاؤها مشافهة أو طريق الكتابة ، أو بأية وسيلة شأنها إعلام الغير بها، ويمكن أن يتم اللجوء للإفشاء بطريقة غير مباشرة ، و لا يشترط أن ينصب على كافة المعلومات بل من الممكن أن يقتصـــر على البعض منها ، أما الاســـتثناءات حول الإفشـــاء فهي تكون في الحالات التالية:[125]

- وجود نص قانوني يبيح الإفشـــاء ؛ فقد ورد في التشـــريعات المقارنة نصـــوص تبيح إفشـــاء المعلومات في حالات خاصة ولجهات معينة.

- الإبلاغ عن الجرائم : فالقانون يبيح إفشـــاء الجرائم في حال كان الغرض الإبلاغ عن الجرائم ومنع إرتكابها كما هو الحال لمزودي الخدمات فقد ألزمه القانون تقديم المعلومات للسلطات التحقيق في الجرائم.

- موافقة الشـــخص المعني بالبيانات وقد تكون الموافقة ضـــمنية وقد يشـــترط القانون في بعض الحالات أن تكون الموافقة صريحة على إفشاء المعلومات ومشاركتها، كما لا يجوز استخدام هذه البيانات لأغراض دعائية إلا بموافقة صريحة وخاصة من المعني بالأمر أو ورثته أو وليه.[126]

---

[125] عائشة غزيل ، مرجع سابق ، ص 23

[126] عبد القادر عميمر ، الحماية الجنائية للحق في الحياة الخاصة في البيئة الرقمية، جامعة الحسن الأول ، المغرب ، 2018، ص 82

فقد اشترط المشرع المصري على ضرورة توافر عدة شروط للسماح بجمع البيانات الشخصية ومعالجتها ، وذلك لتعدد صور الانتهاكات التي تلحق بالبيانات الشخصية للأفراد وقد أورد تلك الشروط في المادة الثالثة والمادة السادسة من قانون حماية البيانات الشخصية.[127]

كما وردت ذات الشروط في المادة الخامسة من اللائحة الأوروبية لحماية البيانات الشخصية، وقد حرصت تلك التشريعات على تحقيق المشروعية والإنصاف في حماية البيانات ، باعتبار أن كافة العمليات لا يجب أن تتم كما أسلف القول سابقاً ، إلأ بالموافقة الصريحة من قبل الشخص المعني بالبيانات ، ولأغراض مشروعة ومحددة ومعلنة لذلك الشخص ، مع ضمان أمن وسلامة تلك البيانات، وأن تكون سليمة وصحيحة ، ويتم معالجتها بطريقة مشروعة ، دون استخدام للوسائل الاحتيالية.[128]

وبهذا يتضح أن القوانين يجب أن توفر إلى جانب الحماية الموضوعية للحق في الخصوصية الرقمية ، الحماية الإجرائية ، و إيجاد توازن بين تبني القواعد الإجرائية لمكافحة الجرائم المعلوماتية وبين تكريس الحق في الخصوصية عبر الفضاء الرقمي.

**المطلب الثاني : حماية الحق في الخصوصية الرقمية في التشريعات المقارنة**

أمام المخاطر المعلوماتية تدخلت بعض الأنظمة التشريعية لحماية الحق في الحياة الخاصة ، كما خصصت نصوصاً عقابية عن كل مس بهذا الحق، ومن الأنظمة القانونية الرائدة في هذا المجال النظام التشريعي الفرنسي الذي نص في المادة الأولى من القانون رقم ( 78-17) الصادر في 1978/1/06 المتعلق بالمعلومات والملفات والحريات على : " أن المعلومات في خدمة الفرد، ويجب أن لا تمس بحقوق الإنسان، وبالحياة الخاصة، وبالحريات الفردية والعامة."

وأكدت المادة ( 6) من هذا القانون هذه الحماية، حيث اشترطت أن تجمع وتعالج البيانات الشخصية الخاضعة للمعالجة بطريقة مشروعة وقانونية ولغاية معينة وصريحة ومشروعة كذلك، وان لا تتم المعالجة بعد ذلك إلا من اجل هذه الغاية المحددة لها، وفي هذه الحالة يجب أن تكون صحيحة وكاملة، وان اقتضى الحال معينة، وان تحفظ بشكل يمكن من إظهار شخصية الفرد المعني بالأمر، ولمدة لا تفوق المدة الضرورية لتحقيق الغاية التي جمعت وعولجت من اجلها، أما المادة (7) ، فاشترطت أن تسبق أية معالجة للبيانات الشخصية الحصول على موافقة الشخص المعني بهذه البيانات، وأن توفر شروط أخرى كاحترام التزام قانوني مفروض على المسؤول عن

[127] انظر المادة 3 من الفصل الثاني والمادة 6 من قانون حماية البيانات الشخصية المصري.
[128] المادة 6 من اللائحة الأوروبية لحماية البيانات الشخصية.

المعالجة ، أو حفظ الحياة الخاصـــة للفرد المعني ، أو تنفيذ خدمة عامة من طرف المســـؤول عن المعالجة أو مستقبلها بشرط مراعاة مصلحة الفرد المعني إلى جانب الحقوق والحريات الأساسية.

وفي المادة (35) من ذات القانون ، فقد فرضت على المسؤول عن المعالجة اتخاذ كل الاحتياطات الضـرورية للحفاظ على البيانات الشـخصـية، وعدم إفشـائها للغير والحيلولة دون تغيير شـكلها أو الإخلال بها أثناء المعالجة، أما المادة ( 36) ، فقد نصـت على منع حفظ البيانات الشـخصـية بعد المدة المحددة ما عدا أن تكون من أجل غايات إحصـــائية أو علمية أو في حالة ترخيص الفرد، أو رخصة اللجنة الوطنية للمعلوماتية والحريات.

كما أعطت المادة( 39) للفرد حق مسـاءلة القائمين على معالجة بياناته الشـخصـية عن نوعية هذه البيانات والغاية من معالجتها وعن الأشخاص المستقبلين لهذه البيانات، كما يمكن له الحصول على نسخة من هذه البيانات.

ونصـــت مواد الباب الثالث على تشـــكيل لجنة إدارية مســـتقلة تســـمى "اللجنة الوطنية للمعلومات والحريات"

وهي مكلفة بمراقبة تنفيذ أحكام القانون رقم( 78-17 ) ،وقد حددت المادتان( 6) و(7) ، طريقة مراقبتها والعقوبات التي يمكن أن تقررها.

وقد أورد المشرع الفرنسي ، صوراً لجرائم تشكل اعتداء على الحق في الخصوصية، ومنها التقاط وتسـجيل الأحاديث الخاصـــة كما نصـــت المادة( 1/368) من قانون العقوبات الفرنســـي الجديد، والتي عدلت بالمادة (226/ 1) ، وجريمة التقاط الصـور الخاصـة التي وردت في المادة( 2/368 ) ، وعدَلت بالمادة 2/226 من قانون العقوبات الفرنسي.

كما أكدت أحكام القضـــاء الفرنســـي من خلال صـــدور أحكامها المختلفة على تأكيد الحق في الخصـوصـية، وقد أقرت المحكمة في أحد أحكامها على أنه من الضـروري أن يحصـل المصـور على موافقة الشـخص قبل قيامه بنسـخ الصـور الأصـلية أو عرضـها وألا كان الفعل يشـكل اعتداء على الحق في الصورة.[129]

هذا ويؤسـس قانون حماية البيانات المصـري رقم 151 لسـنة 2020، الإطار الذي يحدد العلاقة بين المعني بالبيانات من جهة، ومسـتخدمي البيانات من جهة أخرى، كالحائز والمتحكم والمعالج، وذلك من خلال تفنيد حقوق المعني بالبيانات وشـــروط جمع ومعالجة البيانات، والتزامات المتحكم والمعالج، وإجراءات إتاحة البيانات الشـخصـية، وطبيعة اسـتخدام البيانات الشـخصـية الحسـاسـة،

[129] عبد الناصر عجالي، مرجع سابق ، ص 117

وكذلك البيانات الشخصية عبر الحدود، واستخدام البيانات الشخصية في التسويق الإلكتروني المباشر، كما يؤسس القانون بدايةً لإنشاء مركز حماية البيانات الشخصية الذي تتحدد مهامه في الرقابة على إنفاذ قانون حماية البيانات الشخصية وإصدار التراخيص والتصاريح والاعتمادات لمزاولة الشركات، وجمع ومعالجة بيانات المستخدمين، كما يخصص القانون حق الضبطية القضائية لأفراد معينة من المركز، ويحدد كذلك الجرائم والعقوبات في الفصل الأخير من القانون.[130]

كما حدد القانون شروطاً لمشروعية معالجة البيانات الشخصية ، حيث نصت المادة( 6 ) من القانون المذكور عدة مفترضات تحدد التزامات معالج البيانات والمتحكم، وعلى رأس هذه الالتزامات يأتي التزام كل من معالج البيانات والمتحكم حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ مركز حماية البيانات الشخصية خلال اثني وسبعين ساعة[131]،وعلى المركز اتخاذ الإجراءات اللازمة للحفاظ على سرية البيانات.

كما أجاز القانون للشخص المعني بالبيانات ولكل ذي صفة أن يتقدم إلى حائز البيانات أو المتحكم أو المعالج بطلب يتعلق بممارسة حقوقه المنصوص عليها في القانون المذكور أعلاه، كما أتاح القانون للشخص المعني بالبيانات الشخصية مع عدم الإخلال بحقه في اللجوء إلى القضاء ، ولكل ذي صفة ومصلحة مباشرة أن يتقدم بشكوى بشأن انتهاك حقوقه على بياناته الشخصية ،[132]( المواد 32، 33) من القانون.

الدستور المصري حظر إفشاء أسرار الخطابات والاتصالات ، حيث نصت المادة ( 11 ) من دستور عام 1923 على أن : " لايجوز إفشاء أسرار الخطابات والتلغرفات والمواصلات التلفونية ألا في الأحوال مالبينة في القانون " ، كما جاء دستور عام 1930 مؤكداً على كفالة حرمة الحياة الخاصة في المادة الرابعة ، ثم جاء دستور عام 1956 وكفل الحماية لحرمة الحياة الخاصة ، بالأضافة إلى دستور 1971 التي عزز وكرَس الحماية للحريات الشخصية وحرمة الحياة الخاصة ، فقد نصت المادة( 41 ) من الدستور على أن : " الحرية الشخصية حق طبيعي، وهي مصونة لا تمس، وفيما عدا حالة التلبس لا يجوز القبض على أحد أو تفتيشه أو حبسه أو تقييد حريته بأي قيد أو منعه من التنقل إلا بأمر تستلزمه ضرورة التحقيق وصيانة أمن المجتمع ويصدر هذا الأمر من القاضي المختص أو النيابة العامة وذلك وفقاً للقانون ويحدد القانون مدة الحبس الاحتياطي "، وقد

130 الاء كليب ، قانون حماية البيانات المصري في ضوء المعايير الدولية ، مرجع سابق ، ص 9
131 قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.
132 انظر المواد 32، 33 من قانون حماية البيانات المصري رقم لسنة 2005.

كرست هذه المادة وأكدت أن الحرية الشخصية حق دستوري مصون لا يجوز المساس به كقاعدة عامة.[133]

وقد نص الدستور المصري لعام 1970 أيضاً على حرمة الحياة الخاصة وذلك في المادة ( 45) ، حيث نصـــت على : " لحياة المواطنين الخاصـــة حرمة يحميها القانون والمراســـلات البريدية والبرقية والمحادثات التليفونية وغيرها من وســـائل الاتصـــال، حرمة وســـريتها مكفولة ولا يجوز مصـــادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضـــائي مســـبب ولمدة محددة وفقاً لأحكام القانون".[134]

وفي المشـرع الجنائي المصـري رقم 37 لسـنة 1972 ،فإن المشـرع قد أضـاف مادتين جديدتين لقانون العقوبات وهما المادة( 309) و المادة (309 /أ ) ، وقد حظر فيهما أفعال الاعتداء على حرمة الحياة الخاصـــة للأفراد وفرض عقوبات على من يرتكب الجريمة المنصـــوص عليها في المواد سالفة الذكر، وجاء نص المادة ( 309 ) مكرر على أنه : " يعاقب بالحبس مدة لا تزيد على سـنة كل من اعتدى على حرمة الحياة الخاصـة للمواطن ، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضا المجني عليه" وهي:[135]

- اسـتراق السـمع أو سـجل او نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريف التليفون.

- التقاط أو نقل من خلال الأجهزة أياً كان نوعه صـورة شـخص في مكان خاص ، فإذا صـدرت الأفعال المشـار إليها في الفقرتين السـابقتين أثناء اجتماع على مسـمع أو مرأى من الحاضـرين في ذلك الاجتماع فإن رضاء هؤلاء يكون مفترضاً.

كما يعاقب بالحبس الموظف العام الذي ارتكب أحد الأفعال المبينة بهذه المادة اعتماداً على ســـلطة وظيفته ، ويحكم في جميع الأحوال بمصـــادرة الأجهزة وما يكون قد اســـتخدم في الجريمة ، كما يحكم بمحو التسجيلات المتصلة عنها.

المشرع الأردني عزز مفهوم الحريات في الدستور والتشريعات، فقد نص الدستور الأردني على حريـة الرأي والتعبير في نص المـادة( 15 فقرة 1 )، والتي جـاء فيهـا : " حريـة الرأي والتعبير مكفولة ولكل أردني أن يعرب عن رأيه بالقول والكتابة والتصوير وسائر وسائل التعبير بشرط أن لايتجاوز حدود القانون."[136]

---

133 مهنا عطية، الحق في الحرية الشخصية، المجلة الجنائية ، دون دار نشر، مصر ، 1997، ص 152

134 أحمد فتحي سرور ، مرجع سابق ، ص 30

135 د. فوزية عبد الستار ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، مصر، 1986، ص 279

136 أشرف الراعي ، حق الحصول على المعلومات في التشريع الأردني ، مركز الأردن الجديد للدراسات، عمان، 2009، ص 25

كما أكد الميثاق الوطني الأردني الصـــادر عام 1991 على حرية التعبير وقد جاء فيه : " تعتبر حرية الفكر والراي والاطُّلاع حقاً للمواطنين كما هي للصـــحافة وغيرها من وســـائل الإعلام والاتصـال الوطنية، وهي حرية ضـمنها دسـتور ولا يجوز الانتقاص منها أو انتهاكها ".[137] ونجد أن الميثاق نص على حث الحصـــول على المعلومات بصـــورة مباشـــرة وصـــريحة ، وأكد حق المواطنن في الحصـــول على المعلومات وتناقلها ، وأدرجه صـــمن حرية الفكر وحرية الرأي والتعبير وهي حقوق أساسية كفلتها المواثيق والمعايير الدولية .[138]

جديرُ بالذكر أن المشرع الأردني يعد أول من أصدر قانوناً لضمان الحق في الوصول للمعلومات بين البلاد العربية، فقد تم نشر هذا القانون في الجريدة الرسمية بعد إقراره وصدور الإرادة الملكية بتاريخ 2007/6/17، تحت اسـم ( قانون ضـمان حق الحصـول على المعلومات) ، وهدف هذا القانون ضـمان حصـول المواطن على المعلومات التي يطلبها ، لكن تبينت الدراسـات والآراء في الأردن أن هذا القانون لم يعمل على تحقيق الأسباب التي أنشئ من أجلها والتي كانت خلف إقراره، من تسـهيل الحصـول على المعلومات، وخاصـة من الحكومة إلى المواطنين والصـحفيين بصـورة خاصة باعتبارهم أكثر استعمالاً للقانون، كما تبين أن هذا القانون لايتوافق مع المعايير الدولية.[139] وفي عام 2015 ، أصـــدر المشـــرع الأردني قانون الجرائم الإلكترونية رقم 27 لســـنة 2015، وتناول مسـألة الخصـوصـية المعلوماتية وحق الوصـول إلى المعلومات في أكثر من مادة محاولاً منـه أن يوفق بين هذين الحقين ، ففي نص المـادة (12 فقرة أ ) قد تنـاولـت حمـايـة المعلومـات المتعلقة بالأمن الوطني أو العلاقات الخارجية للمملكة والسلامة العامة والاقتصـاد الوطني وفرض عقوبة الحبي بمدة لا تقل عن أربعة أشـــهر وغرامة لا تقل عن (500) دينار أردني ولا تزيد عن (5000) دينار أردني،كما شـدد العقوبة في الفقرة ب في حالة كان القصـد من الدخول هو إتلاف أو تدمير أو تغيير أو تعديل المعلومة بغرامة لا تقل عن (1000) دينار أردني ولا تزيد على (5000) دينار.[140]

كذلك نظم القانون ذاته حركة موظفي الضـــابطة العدلية حيث أوجب عليهم القانون في المادة (13 فقرة أ ) [141]الحصـول على إذن من المدعي العام المختص أو من المحكمة المختصـة بالدخول إلى أي مكان تشـير الدلائل إلى اسـتخدامه لارتكاب أي من الجرائم المنصـوص عليها في هذا القانون،

---

[137] انظر الميثاق الوطني الأردني لسنة 1991.
[138] أشرف الراعي ، المرجع السابق، ص 27
[139] عمرو حسبو ، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، عمان، 2000، ص167
[140] انظر قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015 ، المادة 12.
[141] انظر قانون الجرائم الالكترونية الأردني ، المرجع السابق ، م 12 ف أ

كما أجاز لهم تفتيش الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل إلى استخدامها لارتكاب أي من تلك الجرائم وعليهم أن ينظموا محضراً بذلك ويقدموه إلى المدعي العام المختص.[142]

كما تناولت المادة (12) من قانون جرائم أنظمة المعلومات لسنة 2010، أهم الأحكام الإجرائية والمتعلقة بإجراءات الضابطة العدلية كالتفتيش والدخول وضبط أجهزة الحاسب الآلي ومحتوياته، والحكم بمصادرة هذه الأجهزة من قبل المحكمة ، إذ تعالج هذه المادة أهم القواعد الإجرائية الخاصة بجرائم أنظمة المعلومات كالتفتيش والضبط وهي أهم المسائل ويجب مراعاتها حتى لا تنتهك الحق في الخصوصية حيث جاء في نص المادة (12) :" (أ. مع مراعاة الشروط والأحكام في التشريعات النافذة ومراعاة حقوق المشتكى عليه الشخصية، يجوز لموظفي الضابطة العدلية، بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة ، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون ، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج والأنظمة والوسائل التي تشير الدلائل في استخدامها لارتكاب أي من تلك الجرائم، وفي جميع الأحوال على الموظفي الذي قام بالتفتيش أن ينظم محضراً بذلك ويقدمه إلى المدعي العام المختص.

ب. مع مراعاة الفقرة (أ) من هذه المادة ومراعاة حقوق الآخرين ذوي النية الحسنة ، وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون ، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج والأنظمة والوسائل المستخدمة لارتكاب أي من هذه الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلة منها والتحفظ على المعلومات والبيانات المتعلقة بارتكاب أي منها.

ج. للمحكمة المختصة الحكم بمصادرة الأجهزة والأدوات والوسائل وتوقيف أو تعطيل عمل أي نظام معلومات أو موقع الكتروني مستخدم في ارتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون ومصادرة الأموال المتحصلة من تلك الجرائم والحكم بإزالة المخالفة على نفقة مرتكب الجريمة."[143]

أما المادة 16 من قانون جرائم أنظمة المعلومات أيضا فقد حددت مدى اختصاص المحاكم الأردنية في حال ارتكبت جرائم باستخدام تقنيات المعلومات.

---

[142] بارق منتظر اللامي ، المرجع السابق، ص 44

[143] انظر قانون جرائم أنظمة المعلومات لسنة 2010 ، م 12+ م16 ، https://www.iclc-law.com/

فهذه بعض من التشـريعات المقارنة التي عالجت موضـوع حماية الحق في الخصـوصـية الرقمية والبيانات الشـخصـية، ويظهر من خلال تلك المقارنة أن معظم هذه التشـريعات تناولت الحق بشكل موسع كالتشريع الفرنسي ، وبعضها تناولها بشكل ضمني وغير صريح ، من الملاحظ بأنه ومن المفترض في معظم التشـــريعات أن يتم مراعاة التوازن بين الحق في الحصـــول على المعلومات والحق في الخصـوصـية الرقمية وأن لايسـيطر أحدهما على الآخر بمعنى في الحق الوصـول إلى المعلومات وما بين احترام الحق في خصوصية المعلومات ، وموائمتها للمعايير الدولية.

# الفصل الرابع

# الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني و في ضوء المعايير الدولية

أخذت معظم التشـــريعات الداخلية للدول على عاتقها تأســـيس قواعد حماية لمكافحة جرائم تقنية المعلومات بشـكل عام ، ومحاربة الانتهاكات الواقعة على حق الخصـوصـية في العصـر الرقمي بشكلٍ خاص ، ومن المفترض بان تكون السياسات التشريعية للدول فيما يتعلق بجرائم الانترنت أن يؤسـس على أن المصـلحة التي يحميها القانون هي الحق في المعلومات وفق توازن يتعلق بتدفقها وجمعها وتخزينها، وأن هذه الجرائم هي تحول من ســـلوكيات مادية إلى معنوية ، مما يتطلب أن تكون الحماية مؤسسة على الأهمية المتنامية للقيم المعنوية وسن قواعد تتواءم مع طبيعتها.

من خلال هذا الفصل ستقوم الباحثة بتحليل واقع الخصوصية والبيانات في المشرع الفلسطيني، وتقييم درجة حماية القوانين النافذة للحق في الخصـوصـية الرقمية ، وهل تراعي المعايير الدولية في حالات التدخل بصفة أن فلسطين قد وقعت على الاتفاقيات الدولية واعتبرتها ملزمة لها.

## المبحث الأول: علاقة الخصوصية الرقمية بالديمقراطية وحقوق الإنسان وتحديات الحقوق الرقمية في فلسطين

تعتبر الحقوق الرقمية أو حقوق الانترنت امتداد طبيعي لحقوق الإنســـان في عصـــر الثورة الالكترونية والتطور الرقمي المتلاحق في العالم الواقعي، وهي حقوق أقرتها الأمم المتحدة كما ســبق الذكر، ويعد قرار مجلس حقوق الإنســان في العام 2012، من أبرز القرارات التي تنص على الحقوق الرقمية ، حيث أكد على أن الحقوق التي يتمتع بها البشـر في الحياة الواقعية يجب أن تكون محمية على الانترنت دونما اعتبار للحدود، وبأي وســيلة يختارها الأشـــخاص وأُكد على القرار نفسه خلال العامين 2014 و 2016.

فيما يتعلق بالحقوق الرقمية في فلسـطين فإنها تشـمل : حرية الرأي والتعبير على الانترنت، الحق في الحصـول على المعلومات، الحق في الخصـوصـية، الحق في حماية البيانات، الحق في التحرر من الرقابة، الحق في الأمان الشـخصـي، الحق في الانتصـاف العادل.[144] في هذا المطلب سـيتم

[144] قطاع الاتصالات وتكنولوجيا المعلومات والحقوق الرقمية الفلسطينية "ورقة حقائق"، مركز الميزان لحقوق الإنسان، غزة ، فلسطين ، 2021، ص 3

تحليل واقع الخصوصية وحماية البيانات الرقمية في فلسطين والتحديات التي تواجه هذه الحقوق، والتطرق إلى الحماية الدستورية لهذا الحق وفقاً للمشروع الفلسطيني.

**المطلب الأول: واقع الخصوصية الرقمية في فلسطين**

لقد صاحب ظهور الحاسبات الالكترونية خطورة على الحياة الخاصة للأفراد تمثلت في تهديد هذه الآلة لحقوق الإنسان، وباتت حياته معرضة للأخطار أمام هذه الأجهزة، كما أن النصوص التقليدية في قانون العقوبات سواء العامة أو الخاصة غير كافية لحماية الحياة الخاصة ، وحماية سرية البيانات في مواجهة الحاسبات الالكترونية ، في حال إساءة استخدام البيانات الشخصية .

ومما لاشك فيه بأن وجود قانون للخصوصية وحماية البيانات هو مؤشر قوي يدل على ديمقراطية الدولة وشفافيتها ونزاهتها، أي أنه إذا توفر احترام للخصوصية وحماية البيانات، توفر الجو الديمقراطي الذي يحترم حقوق الإنسان والحريات ، ويرتبط مفهوم الحرية بشكل وثيق بالخصوصية وحماية البيانات ، فاحترام حقوق الانسان والحياة الخاصة هو مبدأ أساسي في مفهوم الحرية وحقوق الإنسان.

كما أن مفهوم الخصوصية بشكلها العام مرتبط بمدى شفافية النظام، والحوكمة الرشيدة ، بل مرتبط بمنظومة الحقوق الإنسانية كافة،لأن جميع الحقوق مرتبطة بالبيانات، والحقوق لا تجزأ، ومن المفترض أن قانون الخصوصية وحماية البيانات يفترض أن يهيمن على منظومة الحقوق الإنسانية ويبني نظاما قائماً على النزاهة كما أشارت إليه المبادئ التوجيهية لأمم المتحدة فيما يتعلق بالخصوصية الرقمية وحماية البيانات الشخصية.

إذ أنه وفي هذا الأطار لابد من إيجاد مجموعة من القواعد التي تشتمل على الآليات التي تنظم أعمال جمع البيانات وتخزينها ومعالجتها ونقلها، وكذلك وضع القواعد التي تنشئ للأفراد الحقوق المعلوماتية المتعلقة بالكمبيوتر ونظم المعلومات وشبكة الانترنت ، والتي يتم من خلالها تنظيم الدخول إلى المواقع الخاصة بهم وحقوق أصحابها بسلامتها وصحتها وقدرتهم على تغييرها وتعديلها، بالإضافة إلى الحماية الإدارية والتنظيمية والمدنية ، بحيث يشكل في مجموعها القانون الذي يقرر الحقوق ويرتب الالتزامات على كل أفراد المجتمع بما يتعلق بالبيانات والمعلومات الخاصة بالحواسيب والشبكات ووسائل الاتصال الحديثة.

يمكن القول بأن التشريعات التي قطعت شوطاً في حماية الخصوصية إنما ذهبت إلى توفير الإطار التشريعي الذي يكفل الحق في المعلومات ، وحرية تدفقها وانسيابها ، والحق في الحياة الخاصة، ومبدأ عدم الاعتداء على البيانات الشخصية، وقد اشتملت قواعدها حماية الحياة الخاصة للأفراد

من مخاطر جمع وتخزين ومعالجة واستخدام هذه البيانات والتي يمكن أن يتم جمعها من قبل الهيئات ومراكز المعلومات، وقد تضمن بعضها قيوداً على نقل البيانات خارج الحدود وغير ذلك من القواعد التي يتلخص مضمونها في حماية امتلاك الشخص وتحكمه في معلوماته.[145]

ولاحقاً لانضمام فلسطين لسبع اتفاقيات دولية أساسية لحقوق الإنسان ، من بينها العهد الدولي الخاص بالحقوق المدنية و السياسية من دون أي تحفظات في العام 2014 ، فقد أصبح واجباً على السلطات في فلسطين اتخاذ كافة التدابير الممكنة ، بما فيها إصدار التشريعات لتنفيذ جميع التزاماتها تجاه الحقوق والحريات الأساسية بموجب العهد الدولي ، وبالرغم من نص القانون الأساسي الفلسطيني المعدل لسنة 2003 على الحق في الخصوصية في المواد (10 ) و( 17 )، إلا أنه لغاية اليوم لم يتم إصدار قانون فلسطيني شامل ينظم قواعد ومفاهيم الخصوصية ، بما في ذلك الخصوصية الرقمية وحماية البيانات الشخصية ، بحيث يمكِن المواطن الفلسطيني من معرفة حقوقه والتزاماته ، وضمان محاسبة كل من يستغل هذا الحق بوجه غير مشروع وبشكل تعسفي ، دون تمييز أو تفرقة بين أي جهة من الجهات سواء من قبل السلطات العامة أو المؤسسات الخاصة المتعلقة بمزودي الخدمة ، وكل ذلك يتم بصورة تتماشى وتتواءم مع التزامات فلسطين وفقا للاتفاقيات الدولية الموقعة عليها.[146]

وعليه تكمن أهمية وجود قانون فلسطيني ناظم للخصوصية وحماية البيانات، وذلك في فرض تنظيم كامل للتعامل مع الخصوصية والبيانات الشخصية بشكل مفصل، وتوفير رقابة وحماية كاملة، وتوزيع مهام ومسؤوليات واضحة، وهو ما يتفق مع التزام فلسطين بالاتفاقيات الدولية، مثل العهد الدولي الخاص بالحقوق المدنية والسياسية ، ومن جهةٍ أخرى أصبح من غير الممكن المعالجة لحق أساسي للفرد بهذا الحجم من خلال نصوص عامة ، بل يجب وجود قانون وتشريع خاص منسجم مع المعايير الدولية .[147]

وبهذا فإن الخصوصية المعلوماتية ينبغي أن تكون جديرة بالاحترام والحماية،لأن لكل شخص الحق في الأمان والامتلاك، والامتلاك يشير إلى الملكية الخاصة والملكية الفكرية، ولهذا دعت الجمعية العامة للأمم المتحدة جميع الدول إلى مراجعة إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة الاتصالات واعتراض وجمع البيانات الشخصية، وأكدت على ضرورة أن تكفل الدول

---

145 د.عبد اللطيف، ربايعة، الجرائم الالكترونية " التجريم،والملاحقة والإثبات"، بحث مقدم إلى مؤتمر الجرائم الالكترونية ، جامعة النجاح الوطنية، فلسطين ، 2016، ص 19

146 كاثرين ، أبو عمشة، ورقة موقف بشأن مسودة قانون حماية البيانات الشخصية من منظور حقوقي ،المركز العربي لتطوير الإعلام الاجتماعي – حملة - ، فلسطين ، 2023، ص 5

147 محمد، الهندي،نفاذ قانون الجرائم الالكتروني"المجتمع المدني وانكفاء الدور،المركز الفلسطيني لأبحاث السياسات والدراسات الاستراتيجية "مسارات"، فلسطين، 2018.

التنفيذ الكامل والفعال لالتزاماتها بموجب القانون الدولي لحقوق الإنسان ، كما تضمنت القرارات الصادرة عن الجمعية العامة للأمم المتحدة بموجب المقرر الخاص لحقوق الإنسان، توصيات بمراجعة الإجراءات والممارسات الحالية والتشريعات الوطنية، كما نصت المادة 12 من الإعلان العالمي لحقوق الإنسان والمادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية على أنه " لا يجوز إخضاع أحد لتدخل تعسفي أو غير قانوني في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته.." وهذا ما التزمت به 167 دولة ، كما تنص أيضا على أن " لكل شخص الحق في حماية القانون من مثل هذه التدخلات أو تلك الحملات "، في حين أن الحق في هذه الخصوصية ليس مطلقاً، على أن تكون هذه القيود مدرجة بشكل واضح في القانون وأن لا تكون تعسفية بأي شكل.[148]

ومما لا شك فيه بأن خصوصية الحال الفلسطينية تتطلب جهداً أكبر لوضع فلسطين على خارطة الانترنت، والاستثمار فلسطينياً في قوة الرواية الرقمية، لتشكيل محتوى وخطاب إعلامي رقمي للقضية الفلسطينية، وللضغط على إدارة المحتوى في بعض المنصات الكبرى لتبني سياسات منصفة وعادلة تحترم مبادئ حقوق الإنسان والقانون الدولي.

وإن واقع الجرائم الالكترونية وملاحقتها في فلسطين يعتبر حالة مختلفة عن واقع هذه الجرائم في مختلف الدول بسبب وقوعها تحت الاحتلال الإسرائيلي الذي يسيطر على سماء وفضاء فلسطين الالكتروني سيطرة تامة، مما يضفي خصوصية عند ملاحقة هذه الجرائم.

و في ما يتعلق بحماية خصوصية الفلسطينيين وسيطرة الاحتلال الإسرائيلي فتشير الدراسات حول الخصوصية وحماية البيانات في فلسطين أن تبني قانوناً لحماية البيانات لن يوفر سوى مستوى محدود من الحماية، نظرا لخضوع البنية التحتية الخاصة بتكنولوجيا المعلومات والاتصالات الفلسطينية للسيطرة الكاملة الإسرائيلية، منذ احتلالها للأراض الفلسطينية، ورغم توقيع اتفاقية أوسلو للسلام عام 1993، إلا أن السلطات الإسرائيلية لاتزال تسيطر على المعلومات والاتصالات والموجات الكهرومغناطيسية، بالإضافة إلى تحكمها في عمليات استيراد وتركيب أي معدات، من قبل شركات الاتصالات الفلسطينية ومقدمي خدمات الانترنت، وذلك لدواعِ أمنية، وتستخدم تقنيات مراقبة وتجسس، أعدت خصيصاً للتجسس على الأفراد ومتابعتهم ،إلى جانب تعاون الشركات

[148] عصام عابدين ، ولاية المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، مؤسسة الحق، رام الله ، فلسطين، 2018، ص 64

العالمية التي تدير منصـــات التواصـــل الاجتماعي مع وحدات الأمن الإســـرائيلية بكل ما يخص المستخدم الفلسطيني.[149]

وبالرغم من التحديات التي تواجه الخصـــوصـــية الرقمية في فلســـطين ، إلا أنه قد ظهر اهتمام وحرص المشـرع الفلسـطيني بفرض الحماية المسـتحقة للحق في الخصـوصـية، من خلال القانون الأســـاســـي الفلســـطيني وذلك من خلال واجب الدولة في التكفل بحماية هذه الحق ، مع تســـخير التشـــريعات المتعلقة بهذا الحق لعدم المســـاس بحرمته ، من خلال القرار بقانون المتعلق بالجرائم الإلكترونية ، أو من خلال قرار مجلس الوزراء المتعلق بحماية البيانات الشخصية ، لكن و بالرغم من إقرار هذه القوانين لكن لازالت تواجه الحقوق الرقمية في فلسطين انحراف في استخدامات هذه التقنيات الرقمية ، لذلك من الضروري وضع تجريمات تعنى بحماية الخصوصية الرقمية للأفراد بشـكلٍ مباشـر ، وتسـتجيب للتطورات التكنولوجية المتلاحقة ، كذلك فإنه لا بد من اتخاذ التدابير اللازمة بهذا الخصـــوص لضـــمان الوقاية والحماية والأمان للأفراد، و تطبيق برامج حماية في المجتمع الرقمي، مثل عمل نســـخة احتياطية للبيانات ، وبرامج مكافحة للفيروســـات والاختراق وغير ها من الإجراءات في العالم الرقمي، فالمواطن الرقمي لا بد له من أن يتخذ الاحتياطات الأمنية اللازمة لحماية بياناته وخصـــوصـــيته من أي غزو خارجي، على الرغم من أن شـــبكات الاتصالات والانترنت الآمن لا تعمل بالمعايير الآمنة عالمياً في فلسطين، فالمواطن الفلسطيني كما ذكرنا سابقا يتهدد أمنه الرقمي خطران، منها ما هو متعلق بالسياسات الفلسطينية ، والاخر متعلق بالانتهاكات الإسـرائيلية في محاولة فرض الرقابة على المحتوى المنشـور، وإلحاق العقوبات على من يخالف تلك السياسات.[150]

**المطلب الثاني : الحماية الدستورية للحق في الخصوصية في فلسطين**

بالحديث عن الحماية الدسـتورية للحق في الخصـوصـية ، فيعتبر القانون الأسـاسـي المعدل لسـنة 2003 ، هو الأســاس الدســتوري للتشـريعات والتدابير الوطنية ، فهو ينظم شـكل الدولة وطبيعة نظامها وسلطاتها الثلاث والفصل بينها ، كما وينص على الحقوق والحريات في الباب الثاني منه ، وقد جاء فيه أن حقوق الإنسـان وحرياته الأسـاسـية ملزمة وواجبة الاحترام في المادة العاشـرة من الباب الثاني ، وأن الاعتداء على الحقوق والحريات التي يكفلها جريمة لا تســـقط الدعوى الجنائية

[149] مروة ،فطافطة و ديما،سمارو ،حماية البيانات في منطقة الشرق الأوسط وجنوب افريقيا،أكسس ناو،2021.
[150] مأمون، مطر، المرجع السابق ، ص 45

ولا المدنية الناشئة عنها بالتقادم وتضمن السلطة الوطنية تعويضاً عادلاً لمن وقع الضرر عليه كما ورد في نص المادة 32 من القانون الأساس.[151]

وقد أشار القانون الأساسي إلى الحق في الخصوصية في المادة 32 من الباب الثاني تحت مسمى " حرمة الحياة الخاصة"[152] ، بالإضافة إلى ذلك نص القانون الأساسي صراحة على حماية بعض مكونات الحق في الخصوصية ، كخصوصية الجسد ، وخصوصية الحيز المكاني"المسكن" وهي الأحكام المتعلقة بالتفتيش كما ورد في المواد 11 و16 و17 من القانون الأساسي والتي سنأتي على ذكرها لاحقاً.

وبناءً على ذلك فمن الملاحظ أن القانون الأساسي لا ينص على حماية شاملة لعناصر الحق في الخصوصية ، بما فيها خصوصية المعلومات والقضايا المتعلقة بالخصوصية في العصر الرقمي ، لكن ومما لاشك فيه بأن نص المادتين 10 و32، يشكلان أساساً دستورياً لحماية الحق في الخصوصية ، وخاصة إذا ما تم تطبيق المعايير الدولية المتعلقة بالحق في الخصوصية الرقمية والمتعلقة بمراقبة الاتصالات وأشكال التدخل الأخرى بهذا الحق ، لكن وبالنظر إلى نصوص المواد 11 و16 و17 المتعلقة بحالات التدخل في الخصوصية التي يجب أن تكون مشروطة بأمر قضائي وفقاً لأحكام القانون ، وفي هذه الحالات على القانون اشتراط وجود الأمر القضائي واعتباره قيداً يفرض على الحقوق والحريات، وعليه فإنه من المهم توافر الاستقلالية والحيادية والوقاية من التدخل غير القانوني أو التعسفي في الخصوصية، وهذه المعايير تتوفر في السلطة القضائية دون غيرها ، و يكون متمثلاً في استقلال القضاة وحيادهم، وفي هذا الخصوص عبَرت اللجنة المعنية لحقوق الإنسان : "الشئ الطبيعي في الممارسات السليمة للسلطة القضائية هو أن تمارس تلك السلطة على يد جهة مستقلة وموضوعية وغير متحيزة في ما يتعلق بالقضايا التي تعالجها "[153]، وفي هذا السياق لا تعتبر اللجنة المعنية المدعي العام موظفاً مخولاً لممارسة السلطة القضائية.[154]

وعليه يجب على المشرع أن يلتزم بإطار الضوابط الدستورية، ولا أن يفرض قيوداً على الحريات تجعل تنظيمها إلى حد مصادرتها أو إهدارها ، لأن الحق في الخصوصية حق دستوري كفله القانون الأساسي كما ذكر سابقاً ، بالإضافة إلى أن دولة فلسطين عضو في العهد الدولي الخاص

---

151 نشر القانون الأساس المعدل لسنة 2003 في مجلة الوقائع الفلسطينية بتاريخ 2003/3/19.

152 انظر المادة 32 من القانون الأساس الفلسطيني المعدل لسنة 2003

153 اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 35 على المادة 9 من العهد الدولي الخاص بالحقوق المدنية والسياسية المعنية بالحق في الحرية والأمان الشخصي

154 عمار ،جاموس، الحق في الخصوصية بين المعايير الدولية والواقع الفلسطيني،الهيئة المستقلة لحقوق الإنسان، فلسطين ،2022،ص 32

بالحقوق المدنية والسياسية الذي يكفل الحق في الخصوصية في جميع الأحوال ، أي فعلياً وعبر الفضـــاء الرقمي ، وعلى جميع الأفراد والقطاعات والجهات الالتزام بحماية واحترام الحق في الخصوصية بجميع الأحوال .[155]

[155] الدليل الإجرائي لحماية البيانات الشخصية الفلسطينية عبر الفضاء الرقمي ، المركز الفلسطيني لتطوير الإعلام الاجتماعي – حملة - ، 2023، ص 5

## المبحث الثاني: التنظيم القانوني للحق في الخصـــوصـــية الرقمية في التشـــريع الفلسطيني

نظمت القوانين في فلسطين بعض حالات التدخل في الخصوصية مثل التفتيش وضبط المراسلات والمراقبة، كما تطرق القرار بقانون المتعلق بالجرائم الالكترونية إلى الخصوصية وحماية البيانات الشخصية ، بالإضافة إلى القرارات بقانون ، فالقانون الأساسي الذي يعتبر هرم التشريعات في الدول، وفي هذا المطلب سوف نستعرض تلك القوانين وارتباط نصوصها وأشكال التدخل في الخصوصية، وذلك لقياس مدى انسجام هذه التشريعات والحماية المخصصة لها مع المعايير الدولية ذات العلاقة.

### المطلب الأول :الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني

بالحديث عن الإطار القانوني للحق في الخصـوصـية في العصـر الرقمي والحماية الجزائية لهذا الحق في التشـريعات الوطنية وكيف تم تناولها وتنظيمها ، نلاحظ أن القوانين النافذة نظمت بعض حالات التدخل في الخصـوصـية مثل التفتيش، وضـبط المراسـلات والمراقبات الإلكترونية إنفاذاً للقوانين الجزائية ، أو لغايات وقائية للمحافظة على النظام العام في فلســطين ، كما تناول القرار بقانون الجرائم الالكترونية المعدل رقم 10 لسـنة 2018 حالات التدخل في الخصـوصـية عبر الوسائل الالكترونية .[156]

عند الحديث عن التفتيش في الجرائم الالكترونية فقد اتجه القرار بقانون الجرائم الالكترونية رقم 10 لسنة 2018 وتعديلاته إلى تفتيش الأجهزة أو أية أدوات لها علاقة بالجريمة أو ضبطها ، فقد نصت المادة 52 فقرة 2 من القرار بقانون على : "إذا أسفر التفتيش عن ضبط أجهزة أو أدوات أو وسائل ذات صلة بالجريمة، يتعين على مأموري الضبط القضائي تنظيم محضر بالمضبوطات ، وعرضـها على النيابة العامة لاتخاذ ما يلزم بشـأنها "،[157] أي انه فيما يتعلق بضـبط المراسـلات وتفتيش الأجهزة الالكترونية، فإنه من الملاحظ أن المراســلات تنطوي على درجة كبيرة من الخصـوصـية نظراً لاشـتمالها في العادة على معلومات شـديدة الحسـاسـية والسـرية تمس الحياة الخاصـــة للمرســـل أو المرســـل إليه أو الغير، وبالتالي يجب إحاطتها بحماية و ضـــمانات تكفل سريتها، ولكن لمَا كان الأمر يتعلق بجريمة ، هنا يجب أن يخضـع مخزن الأسرار هذا لاعتبارات

[156] عمار جاموس ، الحق في الخصوصية بين المعايير الدولية والواقع الفلسطيني ، مرجع سابق ، ص 32
[157] القرار بقانون بشان الجرائم الالكترونية وجرائم الاتصالات وتكنولوجيا المعلومات لسنة 2018 وتعديلاته المادة 2/52

التوازن بين المصـالح الشـخصـية من جهة ، وحقوق الآخرين وحق المجتمع في العقاب من جهة أخرى.

كما جاء في قانون الإجراءات الجزائية الفلسطيني نصوص ناظمة لحالات التدخل في الخصوصية من خلال ضـبط المراسـلات، حيث جاء في المادة 1\51 منه :" على النائب العام أن يضـبط لدى مكاتب البريد والبرق الخطابات والرسـائل والطرود والبرقيات المتعلقة بالجريمة والشـخص المرتكب لها "[158]، وهذا يعني أن المشـرع الفلسـطيني أجاز تفتيش المكونات المادية للحواسـيب ، وضبط أي أدوات لها علاقة بالجريمة ، وفيما يتعلق بالوسائل المعنوية للأجهزة الالكترونية كالبريد الالكتروني والبريد الصـوتي وجواز تفتيشـها ، فقد اتجهت أغلب التشـريعات على ان تكون هذه المكونات محلاً للتفتيش والضبط القضـائي، وقد نص القرار بقانون الجرائم الالكترونية الفلسطيني على تفتيش مكونات الحواسـيب المعنوية ، فقد أجاز لوكيل النيابة أن يأذن بالنفاذ الفوري المباشـر لمأموري الضـبط القضـائي أو من أهل الخبرة إلى أجراء التفتيش فيها بقصـد الحصـول على المعلومات.[159] وهذا ما نص عليه المشرع الأردني والمشرع المصري أيضاً.

وبهذا يتضح أن أحكام ضبط المراسلات تنسحب على المراسلات والخطابات الالكترونية التي تتم عبر وسـائل تكنولوجيا المعلومات ، من خلال القرار بقانون الجرائم الالكترونية رقم 10 لسـنة 2018، الذي نظم حالات التدخل في الخصوصية والوصول إلى المعلومات الشخصية من خلال ضـبط الرسـائل الالكترونية، قد جاء بأحكام مفصـلة ، وبالوقت ذاته تم التراجع فيه عن الضـمانات التي كانت توفرها الماة 1\51 من قانون الإجراءات الجزائية الفلسـطيني، حيث أن النصـوص الواردة فيه تعطي صـلاحية ضـبط الرسـائل الالكترونية وأكثر من ذلك للنيابة العامة، أو من تقوم بانتدابه من مأموري الضبط القضائي ، بعد أن كانت هذه الصلاحية محصورة للنائب العام ، ونص القرار بقانون للجرائم الالكترونية على صلاحية النيابة العامة في الحصول على الأجهزة والأدوات أو الوسائل والبيانات والمعلومات الالكترونية ، وكذلك أعطاها صلاحية ضبط كامل المعلومات أو جزء منها والوسـيلة التي تحتويها، ولم يحدد القرار بقانون درجة خطورة الجريمة التي تسـتدعي مثل هذا التدخل الخطير في الخصـوصـية الرقمية، فبالنظر في المادة 34 من القرار بقانون [160] نجد أنه يمتنع على مأمور الضـبط القضـائي ووكيل النيابة ضـبط الأجهزة الالكترونية والتفتيش في

---

[159] المادة 34 من القرار بقانون الجرائم الالكترونية الفلسطيني نصت على أنه : "يجوز لموظف الضابطة العدلية بعد حصوله على موافقة المدعي العام أو المحكمة المختصة الدخول إلى أي مكان تشير الدلائل إلى استخدامه في ارتكاب أي الجرائم المنصوص عليها في هذا القانون .."

[160] انظر م 34 من القرار بقانون بشأن الجرائم الالكترونية رقم 10 لسنة 2018.

المحادثات التي جرت إلا بعد الحصول على إذن قضائي من قبل النائب العام، لأن المحادثات التي تجري وفق أجهزة الحاسوب الآلي أو حتى وفق المواقع الالكترونية تدخل في عداد الاتصالات السلكية واللاسلكية، أما إذا كانت الجريمة المرتكبة عبر الأجهزة الاكترونية لا تتعلق بمحادثات أو اتصالات وإنما كانت من نوع آخر كأن تكون جريمة تزوير أو احتيال أو التعرض للآداب العامة أو الأخلاق أو الترويج للمخدرات فإنه يكون لوكيل النيابة الحق في الانتقال لمسرح الجريمة وضبط الأجهزة الالكترونية المستخدمة في الجريمة أو إعطاء مأمور الضبط القضائي مذكرة تفتيش عن هذه الأجهزة لضبطها.[161]

ولقد أوضح القرار بقانون أيضا ، أن أمر الحصول على التحفظ العاجل على بيانات حاسوب أو بيانات مرور الاتصالات السلكية واللاسلكية يجوز إصداره ضد: (أ) شخص محدد يحوز أو يتحكم في البيانات المعنية؛ أو (ب) مقدم أو مقدمي الخدمة [162] ، فإذا لم يمتثل الشخص لأمر التحفظ العاجل على بيانات حاسوب محددة أو بيانات مرور الاتصالات السلكية واللاسلكية، يجوز لعضو النيابة العامة أو الشرطة مطالبة المحكمة إصدار قرار بالقبض على الشخص الذي خالف الأمر لمدة زمنية تستمر حتى يمتثل للأمر، أو إلى أن يصبح الامتثال أمراً غير ذي صلة.

كما أن أمر التحفظ العاجل على بيانات الحاسوب أو بيانات مرور الاتصالات السلكية واللاسلكية يمكن أن لزم مزود الخدمة أن يكشف عن مقدر كافٍ من بيانات المرور لتمكين الشرطة والنيابة العامة من تحديد هوية المشتركين ، والمسار الكهرومغناطيسي الذي تم من خلال أو عبره إرسال الاتصالات، كما يجوز للقاضي تجديد أمر التحفظ العاجل على بيانات حاسوب محددة ، أو بيانات متعلقة بالاتصالات طالما كان الأمر ضرورياً.[163]

جدير بالذكر بأن مزود الخدمة يقوم بدور رئيسي في تقديم المعلومات الضرورية للمحقق ، إلا أن إلزام مزود الخدمة بانتهاك الخصوصية وتقديم معلومات خاصة عن المشترك بحاجة إلى اقتناع من قبل النيابة العامة أو القضاء بأن هناك سبب معقول للاعتقاد بأن الجهاز المطلوب التفتيش فيه مثلا يحتوي على دليل يتعلق بالجريمة وإن تقرير ما إذا كان السبب معقولا من عدمه خاضع لتقدير المحكمة أو النيابة العامة.

وأيضا ، فقد قصر المشرع الفلسطيني من خلال قانون الإجراءات الجزائية الفلسطيني، سلطة ضبط الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات المتعلقة بالجريمة وشخص

---

[161] مهدي رضوان ،إجراءات الضبط والتفتيش في الجرائم الالكترونية في النظام القانوني الفلسطيني " رسالة ماجستير" جامعة بيرزيت ، 2023، ص 20

[162] انظرالمادة 31 من القرار بقانون المتعلق بالجرائم الالكترونية رقم 10 لسنة 2018.

[163] مهدي رضوان ، مرجع سابق ، ص 28

مرتكبها بالنائب العام أو أحد مساعديه، أي النواب العامون المساعدون، وبذلك يمتنع على وكيل النيابة أو رئيس النيابة ضبط مثل هذه الخطابات أو الرسائل والجرائد والمطبوعات والطرود والبرقيات .

وعلى ضوء ذلك لا يجوز لوكيل النيابة أو رئيس النيابة أن يضبط إذا ما كان مسرح الجريمة مكاتب البرق والبريد الخطابات والرسائل والجرائد والمطبوعات والطرود والبرقيات وإنما يكون ذلك فقط من قبل النائب العام أو أحد مساعديه، ولكن ماذا لو كان مسرح الجريمة الالكترونية مكاتب البرق والبريد، فهل يمتنع على وكيل النيابة المحقق الانتقال إلى مسرح الجريمة للكشف عليه وضبط الأجهزة الالكترونية؟ هذا وفي ظل أحكام المادة 50 من قانون الإجراءات الجزائية الذي يمنع مراقبة المحادثات السلكية واللاسلكية إلا من قبل النائب العام وبإذن من محكمة الصلح هل يجوز لوكيل النيابة الانتقال إلى مسرح الجريمة الالكترونية وضبط أجهزة الحاسوب الآلي والتفتيش بداخلها؟ باعتقادي وفي ظل القيدين الواردين في قانون الإجراءات الجزائية فإنه يمتنع على مأمور الضبط القضائي ووكيل النيابة ضبط الأجهزة الالكترونية والتفتيش في المحادثات التي جرت إلا بعد الحصول على إذن قضائي من قبل النائب العام، لأن المحادثات التي تجري وفق أجهزة الحاسوب الآلي أو حتى وفق المواقع الالكترونية تدخل في عداد الاتصالات السلكية واللاسلكية، أما إذا كانت الجريمة المرتكبة عبر الأجهزة الاكترونية لا تتعلق بمحادثات أو اتصالات وإنما كانت من نوع آخر كأن تكون جريمة تزوير أو احتيال أو التعرض للآداب العامة أو الأخلاق أو الترويج للمخدرات فإنه يكون لوكيل الذيابة الحق في الانتقال لمسرح الجريمة وضبط الأجهزة الالكترونية المستخدمة في الجريمة أو إعطاء مأمور الضبط القضائي مذكرة تفتيش عن هذه الأجهزة لضبطها.[164]

ففي الجرائم المرتكبة عبر الأجهزة الالكترونية يجب مراعاة قواعد التفتيش الواردة في قانون الإجراءات الجزائية من حيث انتقال وكيل النيابة بنفسه أو إعطاء مذكرة تفتيش صادرة وموقع منه لمأمور الضبط القضائي، وهنا يجب مراعاة البيانات التي نص القانون على ضرورة الاشتمال عليها تحت طائلة بطلانها، وما يعني هنا هو تحديد الغرض من التفتيش، وهذا يفترض في وكيل النيابة المعرفة المسبقة وبدقة عما يريده من التفتيش ، لذلك فان مذكرة التفتيش يتعين ان تكون واضحة في تحديد النظام محل التفتيش ، وإيراد أوسع وصف يغطي ما يعرفه المحقق سلفاً وما يفترض انه يتصل بالمسائل التي يعرفها.

[164] عمار جاموس ، المرجع السابق ، ص37

كما جرَم قانون الجرائم الالكترونية انتهاك الخصوصية وحماية البيانات الشخصية من خلال نص المادة (22) أيضاً، حيث جرم نشر الأخبار أو الصور أو أي تسجيلات صوتية أو مرئية متصلة بالتدخل غير القانوني في خصوصية الأفراد أو الجماعات ، ولو كانت صحيحة ، وأفرد عقوبات على مرتكبي هذه الجرائم حيث نصت المادة 22 على:[165]

1- يحظر التدخل التعسفي أو غير القانوني في خصوصيات أي شخص أو في شؤون أسرته أو بيته أو مراسلاته.

2- كل من أنشأ موقعا أو تطبيقا أو حسابا الكترونيا أو نشر معلومات على الشبكة الالكترونية أو إحدى وسائل تكنولوجيا المعلومات ، بقصد نشر أخبار أو صور أو تسجيلات صوتية أو مرئية ، سواء كانت مباشرة أو مسجلة تتصل بالتدخل غير القانوني في الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة يعاقب بالحبس مدة لا تقل عن سنة، أو بغرامة لا تقل عن ألف دينار أردني، ولاتزيد على ثلاثة آلاف دينار أردني أو ما يعادلها بالعملة المتداولة قانوناً أو بكلتا العقوبتين"

وفي العام 2019 أصدر مجلس الوزراء الفلسطيني القرار رقم 3 لسنة 2019 ، الخاص بحماية البيانات الشخصية الخاصة بالمواطنين الفلسطينيين ، على أن يكون ساري النفاذ في الضفة الغربية وقطاع غزة، والقانون يحتوي على مادتين تنصان على : " 1- يحظر استخدام البيانات الشخصية (المباشرة \غير المباشرة) الخاصة بالمواطنين، متلقي الخدمة من الشركات والمؤسسات المزودة بها لأغراض تجارية، دون الحصول على إذن مسبق منهم، تحت طائلة المسؤولية القانونية، 2- على الجهات المختصة كافة ، كل فيما يخصه ، تنفيذ أحكام هذا ويعمل به من تاريخ صدوره وينشر في الجريدة الرسمية .[166]

فيما يتعلق بهذا القرار المتعلق بحماية البيانات الشخصية للمواطنين، فإنه لا يمكن اعتباره بمكانة القوانين ، إذا يأتي الدستور أولاً ، ثم القوانين ثم النظام والقرارات ، وإنما نص على وقوع الفرد تحت طائلة المسؤولية في حال وقوع أي انتهاك، ولا يمكن معالجة حق أساسي من حقوق الإنسان ومنصوص عليه تحت باب الحقوق والحريات في القانون الأساسي من خلال قرار ، فلا بد من تأصيل الحق ، وتحديد الجهات المخولة والمختصة بمتابعة حماية هذا الحق ، وذلك من خلال تشريع قانون لحماية البيانات الشخصية.[167]

---

[165] انظر قانون الجرائم الالكترونية الفلسطيني رقم 10 لسنة 2018، https://muqtafi.birzeit.edu/

[166] انظر قرار الوزراء رقم 3 لسنة 2019 متاح على الموقع https://muqtafi.birzeit.edu/

[167] عمر أبو عرقوب، مرجع سابق ، 2021، ص 32

من خلال جميع ما سبق ترى الباحثة ضرورة السعي لإيجاد قوانين توائم التطور التكنولوجي الذي يشهده العالم لحماية وتنظيم الخصوصية الرقمية ، وضرورة حماية البيانات الشخصية للأشخاص من أي اختراق بما في ذلك تحديد سياسات الخصوصية الرقمية لكل موقع وخدمة ، وأن تتصف هذه القوانين بالشمول ومعالجة كافة القضايا المتعلقة بالخصوصية الرقمية ، وتحديد الجرائم المتعلقة بها، بالإضافة لوضع عقوبات تتناسب مع خطورة الجريمة ، إذ من الملاحظ أن أحكام القضاء الفلسطيني لا تتناول الحق في الخصوصية، ولا يوجد أحكام متعلقة بهذا الحق وخاصة مع اتساع الاعتداءات والانتهاكات الحق على الخصوصية عبر الوسائل التقنية .

## المطلب الثاني: توافق المعايير الدولية مع الحماية الجزائية للحق في الخصوصية الرقمية في التشريع الفلسطيني

مما لاشك فيه بأن القوانين والتشريعات الخاصة للدول يجب أن تستند إلى المعايير الدولية كأساس ومرجع لها ، كاللائحة العامة لحماية البيانات ، والعهد الدولي للحقوق المدنية والسياسية وغيرها من المعايير والاتفاقيات الدولية الملزمة للدول الموقعة عليها ومنها فلسطين ، وهذا ما سيتم تحليله من خلال هذا المطلب.

### الفرع الأول : طبيعة العلاقة بين التشريعات الفلسطينية والاتفاقيات الدولية

يشكل القانون حاجة ماسة لتنظيم حاجة المجتمعات وتنظيم العلاقة بين الأفراد والجماعات ، هذا ويلتصق الحق في الخصوصية الرقمية ، وذلك وفقاً للتقرير السنوي للمفوض السامي للأمم المتحدة لحقوق الإنسان عن الحق في الخصوصية في العصر الرقمي،[168]ويشتمل التقرير أيضا على الحياة الإلكترونية للأفراد ومساحة البيانات الشخصية التي تقع تحت بند الخصوصية الرقمية، وهذا ما أكد عليه الإعلان العالمي لحقوق الإنسان ، والعهد الدولي الخاص بالحقوق المدنية والسياسية في المادة 17 منه.[169]

وقد شهدت الحالة الفلسطينية تطورات على صعيد إصدار التشريعات والقرارات ، وقد تمثلت بإصدار الرئيس الفلسطيني قرار بقانون الجرائم الالكترونية رقم 16 لسنة 2017، وقد أثار هذا القرار بشأن الجرائم الالكترونية عدة ردود أفعال ، ثم صدر القرار بقانون المعدل بشان الجرائم الالكترونية رقم 10 لسنة 2018 ، والذي أثار أيضا العديد من ردود الأفعال حول انسجامه مع

[168] التقرير السنوي للمفوض السامي للأمم المتحدة حول الحق في الخصوصية ، https://www.ohchr.org/
[169] العهد الدولي الخاص بالحقوق المدنية والسياسية ، https://www.ohchr.org/

الالتزامات الناشئة عن انضمام دولة فلسطين للاتفاقيات الدولية لحقوق الإنسان، ولا سيما العهد الدولي الخاص بالحقوق المدنية والسياسية ، والقرار رقم (68/167) الذي اعتمدته الجمعية العامة للأمم المتحدة في كانون الأول \ديسمبر 2013، بشأن عدم جواز التدخل في استخدام الأفراد للفضاء الالكتروني أي انتهاك الحق في الخصوصية ، فالقرار بقانون بشأن الجرائم الالكترونية الصادر عن السيد الرئيس ينظم الاستخدام الالكتروني ، ويجرم مجموعة من الأفعال الناتجة عن الاستخدام لهذا الفضاء الالكتروني ، إلا أنه يحتوي على العديد من المصطلحات الواسعة والفضفاضة التي تحمل تفسيرات متعددة وأكثر من دلالة ، هذا ما يفسر توسع استخدام الصلاحيات للعديد من الجهات أو التعسف في استخدامها ، بما يؤثر بشكلٍ سلبي على حقوق المواطن وحرياته المكفولة بموجب الاتفاقيات التعاقدية التي أصبحت فلسطين عضواً فيها كالإعلان العالمي لحقوق الإنسان وغيره من الاتفاقيات، التي دعت الدول من خلالها إلى وجوب احترام الحق في الخصوصية وعدم جواز التدخل التعسفي في خصوصياتهم أو ما يتعلق بهم وبمراسلاتهم الخاصة ، وكما أكد عليه أيضاً قرار الأمم المتحدة سالف الذكر، على ضرورة حماية حقوق الأشخاص عبر الفضاء الالكتروني كما الحماية التي يتمتعون بها خارجه ، وضرورة اتخاذ كافة التدابير الكافية لحماية ودعم الحق في الخصوصية وعدم انتهاكها.[170]

[170] التشريع الالكتروني ومدى مراعاة الحقوق والحريات العامة " ورقة موقف " ، مركز الميزان لحقوق الإنسان، غزة ، فلسطين ، 2017، ص 3

**الفرع الثاني : انسجام التشريعات الفلسطينية مع المعايير الدولية للحق في الخصوصية الرقمية**

لقد أحال القانون الأساسي الفلسطيني المعدل لسنة 2003 مهمة سن القوانين إلى السلطة التشريعية وجعلها صاحبة الاختصاص الأصيل من خلال نص المادة (47) [171]من القانون الأساسي الفلسطيني المعدل لسنة 2003، وقد وضع النظام الداخلي للمجلس التشريعي قواعد وآليات العملية التشريعية، كذلك منحت المادة( 43) [172]من القانون الأساسي الفلسطيني رئيس السلطة الوطنية الفلسطيني في حالات الضرورة التي لا تحتمل التأخير في غير أدوار انعقاد المجلس التشريعي الفلسطيني ، صلاحية إصدار قرارات لها قوة القانون ، على أن يتم عرضها على المجلس التشريعي في أول جلسة يعقدها ، لكن لوحظ أن إصدار قرار بقانون الجرائم الالكترونية لم يخضع قبل إصداره للمناقشات من قبل أطراف مؤسسات المجتمع المدني والمؤسسات الحقوقية أو مع أصحاب العلاقة، ليراعي مصالح المجتمع وكفالة الحقوق والحريات المتعلقة بالمواطن الفلسطيني ، وإنما فوجئت به الأطراف في المجتمع الفلسطيني ، فقد نصت العديد من مواده على مصطلحات واسعة فضفاضة عند قياسه بالمعايير والمواثيق الدولية التي انضمت لها دولة فلسطين تكون ذات تأثير على الحقوق والحريات لا سيما الحق في الخصوصية الرقمية.[173]

**- قرارات بقانون بشأن الجرائم الالكترونية**

كما ذكر سابقاً ؛ فلقد أثار نشر القرار بقانون رقم (16) لسنة 2017 بشأن الجرائم الإلكترونية اعتراضات واسعة من قبل مؤسسات المجتمع المدني بشأن الآلية التي جرى فيها مناقشته وإقراره ونشره، حيث أنه لم يتم إشراك مؤسسات المجتمع المدني في مناقشته وبخاصة الأطراف المعنية كالمؤسسات الأهلية، نقابة الصحفيين، نقابة المحامين، والشركات المزودة للإنترنت وغيرها، رغم مطالبة العديد من مؤسسات المجتمع المدني بالاطَلاع عليه ومناقشه قبل إقراره ونشره، وبخاصة في ظل استمرار غياب المجلس التشريعي صاحب الصلاحيات الدستورية الأصيلة في التشريع ، وقد قوبلت تشريعات الجرائم الإلكترونية، باحتجاجات واسعة من قبل مؤسسات المجتمع المدني الفلسطيني، كما وجه المقرر الخاص في الأمم المتحدة المعني بتعزيز وحماية الحق في حرية

---

[171] نصت المادة 47 من القانون الأساسي الفلسطيني المعدل لسنة 2003 على المجلس التشريعي ومهامه ومدته"
1-المجلس التشريعي هو السلطة التشريعية المنتخبة 2- بما لا يتعارض مع أحكام هذا القانون يتولى المجس مهامه التشريعية والرقابية على الوجه المبين في نظامه الداخلي 3- مدة هذه المجس هي المرحلة الانتقالية.

[172] نصت المادة 43 من القانون الأساسي الفلسطيني على :" إصدار القرارات في حالة الضرورة
-1لرئيس السلطة الوطنية في حالات الضرورة التي لا تحتمل التأخير في غير أدوار انعقاد المجلس التشريعي، إصدار قرارات لها قوة القانون، ويجب عرضها على المجلس التشريعي في أول جلسة يعقدها بعد صدور هذه القرارات وإلا زال ما كان لها من قوة القانون، أما إذا عرضت على المجلس التشريعي على النحو السابق ولم يقرها زال ما يكون لها من قوة القانون.

[173] التشريع الالكتروني ومدى مراعاة الحقوق والحريات العامة " ورقة موقف " ، مرجع سابق ، ص4

الرأي والتعبير، ديفيد كاي، مذكرة للحكومة الفلسطينية بتاريخ 16 آب/ أغسطس 2017 عبّر فيها عن قلقه من حجب المواقع الإلكترونية الفلسطينية على شبكة الإنترنت بما يشمل المواقع التي تنتقد أداء السلطة الفلسطينية، ومن تأثير قرار بقانون الجرائم الإلكترونية على حرية الرأي، والإعلام، والحقوق الرقمية، والحق في الخصوصية على شبكة الإنترنت في فلسطين، ومن المصطلحات الفضفاضة والعقوبات القاسية المستخدمة، وتأثيرها على الرقابة الذاتية التي يفرضها الأفراد كما وسائل الإعلام، على أنفسهم، وتأتي في ظل غياب قانون بشأن الحق في الوصول إلى المعلومات، بما لا يتماشى مع المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي انضمت إليه فلسطين بدون تحفظات، وطالب السلطة الفلسطينية باتخاذ جميع الخطوات الضرورية لمراجعة القرار بقانون، وضمان انسجامه مع الالتزامات التي يُرتبها القانون الدولي لحقوق الإنسان. [174]

وعلى ضوء ذلك ردت الحكومة الفلسطينية على مذكرة المقرر الخاص في الأمم المتحدة بشأن الجرائم الإلكترونية في أيلول/ سبتمبر 2017 بمذكرة تضمنت 15 بندا، أكدت فيها على تعهد رئيس دولة فلسطين ورئيس الوزراء بتعديل أيّ مادة تخالف القانون الأساسي أو لا تتواءم مع التزامات دولة فلسطين التي ترتبت بموجب الاتفاقيات والمواثيق الدولية".[175]

فالمواد القانونية في هذا القرار كما ذكر سابقا حملت مصطلحات متعددة الدلالة والتفسير ، وذلك يتعارض مع مبدأ اشتراط علم المخاطب بالقانون، والعلم ليس نشره في الجريدة الرسمية فحسب ، بل هو الفهم والوضوح للمواطن بطبيعة الأفعال المجرمة ، والذي يتطلب توافره في التشريع الجنائي ،لانه يتضمن إيقاع الجزاء على من يتم تجريم أفعاله ، فالمصطلحات الواسعة التي تناولها القرار بقانون على سبيل المثال ( النعرات العنصرية ، سلامة الدولة والنظام العام ، السلم الاجتماعي ، الإضرار بالوحدة الوطنية)، يمكن تكييفها وتطبيقها على نطاق واسع دون تحديد، وهذا ما يتعارض مع التزامات فلسطين بموجب انضمامها للعهد الدولي للحقوق المدنية والساسية، والإعلان العالمي لحقوق الإنسان والمبادئ التوجيهية للحق في الخصوصية ، إذ يمكن للهيئات القضائية أن تقوم بتكييف والتجريم وفقاً للمصطلحات الواسعة المذكورة في القرار بقانون بما يشكل انتهاكا للحقوق والحريات المتعلقة بالمواطن الفلسطيني .[176]

---

[174] واقع الخصوصية وحماية البيانات الرقمية في فلسطين، "دراسة استكشافية "، مركز حملة ، 2021

[175] واقع الخصوصية وحماية البيانات الرقمية في فلسطين، المرجع السابق .

[176] التشريع الفلسطيني ومدى مراعاة الحقوق والحريات، مرجع سابق ، ص 6

وكان القرار بقانون كان قد أدى لاعتقال عشرات الصحافيين وناشطي مواقع التواصل الاجتماعي، وجرى حجب نحو 30 موقعاً إلكترونياً دفعة واحدة بالاستناد إلى قرار بقانون الجرائم الإلكترونية لعام 2017، والتي لا تزال محجوبة، ولا يزال بعض الصحافيين يُحاكمون لغاية الآن بتهم تتعلق بـ"الجرائم الإلكترونية"، ومنذ إعلان الطوارىء بات الصحفيون ونشطاء الرأي يلاحقون من خلال الجرائم الإلكترونية.

بعد المطالبات بتعديل القانون أو إلغائه من قبل مؤسسات حقوق الإنسان ومنظمات المجتمع المدني ، صدر قرار بقانون الجرائم الالكترونية الفلسطيني رقم 10 لسنة 2018 المعدل، ، هذا وبالرغم مما ورد في القانون من تعديلات على القانون السابق إلا أنه ورد بنود تقيد من حرية الرأي والتعبير وتنتهك الحق في الخصوصية ، إذ أنه يستخدم العديد من المصطلحات الواسعة في معظم نصوصه وأحكامه، والتي تتعارض مع مبدأ العلم بالقاعدة القانونية ومبدأ الشرعية القائم على الوضوح التام والتوازن بين التجريم والعقاب، بما يترك مجالاً واسعاً للتأويل والتفسير ، إذ ينبغي أن يقتصر دور الجهات القائمة على تطبيق القانون على التحقق من ارتكاب الفعل المجرَّم من عدمه، وليس إذا كان الفعل في ذاته يشكل جريمة أم لا، حتى يكون المواطن على علم بأن ما يقوم يشكل جرماً أم لا، ومن بين تلك المصطلحات الفضفاضة التي تمس بمبدأ الشرعية ومبدأ العلم بالقاعدة القانونية وبالمعايير الدولية عبارات مثل ؛ المساس بالأداب العامة، تعريض سلامة الدولة أو نظامها العام أو أمنها الداخلي أو الخارجي للخطر، الاعتداء على المبادىء والقيم الأسرية، إثارة النعرات العنصرية، الإضرار بالوحدة الوطنية، الإضرار بالسلم الاجتماعي .... وهذا ما ورد في نص المادة 45 من القرار بقانون ، وتلك الجرائم تخرج أولاً عن مفهوم الجرائم الالكترونية بموجب اتفاقية بودابست، وثانياً لا يمكن إدارجها ضمن القيود الواردة على المادة (19) من العهد الدولي الخاص بالحقوق المدنية والسياسية فيما يتعلق بحرية التعبير عن الرأي .[177]

كما و ينبغي التفريق بين المواقع الإلكترونية "الإعلامية" وغيرها من المواقع في الإجراءات التي يتم اتخاذها في مسار الدعوى الجزائية في الجرائم الإلكترونية، وذلك إعمالاً لنص المادة (27) من القانون الأساسي والتي لا تجيز بالنص الصريح فرض "أية قيود" على وسائل الإعلام إلا بموجب نص في القانون "وحكم قضائي". وكذلك فإن القرار بقانون يتجاوز الأصول والضمانات الواردة في قانون الإجراءات الجزائية فيما يتعلق بمراقبة الاتصالات والمحادثات الإلكترونية وكذلك

[177] د.عصام عابدين ، جهود مؤسسة الحق في مواجهة قرار بقانون الجرائم الالكترونية ، مؤسسة الحق، رام الله ، 2018، ص 39

المعـايير الـدوليـة التي عبر عنهـا المقرر الخـاص المعني بتعزيز وحمـايـة الحق في حريـة الرأي والتعبير وبخاصة في تقريره المقدم إلى مجلس حقوق الإنسان في العام 2013 .

فلا يزال القرار بقانون المعدَل يتيح صـلاحية حجب مواقع إلكترونية كما ورد في نص المادة 39 حول الإذن بحجب المواقع خلال 24 ولمدة سـتة أشـهر قابلة للتجديد وذلك بناءً على طلب النائب العام أو أحد مساعديه صلاحية الطلب من قاضـي الصـلح ، حيث يتم ذلك بإغلاق مواقع الكترونية خلال 24 ســـاعة وتصـــدر المحكمة قرارها في ذات اليوم فيما يتعلق بأية جريمة واردة في قرار بقانون الجرائم الالكترونية ، وذلك خلافاً للمعايير الدولية ،وبخاصة ما ورد في قرار مجلس حقوق الإنسان الصادر عام 2016 والذي أدان بشكل قاطع في بنده العاشر التدابير المتخذة بقصد منع أو تعطيل الوصـــول إلى المعلومات أو نشـــرها على الانترنت، في انتهاك للقانون الدولي لحقوق الإنسان، ويدعو الدول إلى الامتناع عن هذه التدابير ووقفها .

وبالتالي، فإن اللجوء إلى حجب مواقع إلكترونية يتطلب إعمالاً لمبدأ الضرورة والتناسب أن يصدر بموجب حكم قضـــائي نهائي، وليس في مســـار التحقيق، وعلى الجرائم الأشـــد خطورة في القرار بقانون من قبيل الجرائم المنظمة أو استغلال الأطفال في الأعمال الإباحية وليس على كافة الجرائم الواردة في القرار بقانون، وفي ذلك يؤكد المقرر الخـاص المعني بتعزيز وحمـايـة حريـة الرأي والتعبير ؛ بما يلي " يعتبر الحجب الإجباري لمواقع كاملة أو عناوين إنترنت أو منافذ أو شـــبكات أو أنواع معينة من الاسـتخدامات مثل مواقع التواصـل الاجتماعي إجراءً متطرفاً يماثل في شـدته حجب صـحيفة أو مؤسـسـة بث ولا يمكن أن يكون مبرراً إلا بموجب المعايير الدولية وذلك عندما يكون ضرورياً لحماية الأطفال من الاستغلال الجنسي" ، وفي البند السادس المعنون (الوصول إلى الانترنت) يؤكد على ما يلي" يعتبر حرمان الأفراد من الحق في الوصـــول إلى الانترنت كعقاب إجراءً قاســـياً ولا يمكن أن يكون مبرراً إلا عندما لا يكون هناك اي إجراءات أقل تقييداً متاحة وبموجب أمر صـــادر عن المحكمة آخذين في الحســـبان أثر ذلك الإجراء على التمتع بحقوق الإنسـان"، أي أنه ينبغي التعامل مع حجب المواقع الإلكترونية، إعمالاً لشرط الضـرورة والتناسب في المعايير الدولية، ، إذ لا يمكن أن يكون الحجب للمواقع الالكترونية مبرراً إلا بموجب المعايير الدولية.

كما يتجاهل القرار بقانون المعايير الواردة في المبادىء الدولية لتطبيق حقوق الإنســـان فيما يتعلق بمراقبة الاتصـالات لعام 2014 وبخاصـة فيما يتعلق "بإخطار المستخدمين" بصـدور إذن قضـائي بمراقبة اتصـــالاتهم بما يتيح لهم وقتاً كافياً لتمكينهم من الطعن على القرار ، وقد نصـــت المبادىء الـدوليـة على أن التـأخير في الإخطـار ليس مبرراً إلا بـاجتمـاع الظروف التـاليـة وهي: أن يكون

الإخطار من شأنه إفشال الغرض الذي من أجله صُرح بالمراقبة أو أن يؤدي إلى خطر حال وشيك على حياة إنسان، وإصدار الإذن من جهة قضائية كفؤة ومستقلة وقت المراقبة، وإخطار الأشخاص المتاثرين بالقرار فور زوال الخطر، وكذلك الحال بشأن معايير "الشفافية" التي تلزم الحكومة بنشر المعلومات المتعلقة بطلبات المراقبة المقبولة والمرفوضـــة وعدد الأفراد المتأثرين بكل طلب، كما أن القرار بقانون يتجاوز الضـــمانات الواردة في قانون الإجراءات الجزائية الفلســـطين المتعلقة بمراقبة الاتصالات.[178]

جاء في نص المادة 15 من القرار بقانون على أنه :" للنائب العام أو أحد مساعديه أن يأمر بالجمع والتزويد الفوري لأية بيانات بما فيها حركة الاتصـالات أو معلومات إلكترونية أو بيانات مرور أو معلومات المحتوى التي تراها لازمة لمصلحة التحقيقات"، وهذا النص يلاحظ بأنه يستثني القضاء من مراقبة حركة الاتصـــالات والأمر بالجمع والتزويد الفوري للبيانات، إذ ينبغي أن تتم بناء على طلب من النائب العام أو أحد مســـاعديه وقرار من "المحكمة المختصـــة" ، والتي أكدت على أنه لقاضـــي الصـــلح أن يأذن للنائب العام أو أحد مســـاعديه بمراقبة الاتصـــالات والمحادثات الهاتفية للبحث عن الدليل المتعلق بالجريمة، وأن يتم الأخذ بعين الاعتبار "جســـامة الجريمة" في الحالتين بحيث تكون في الجنايات والجنح المعاقب عليها بالحبس مدة لا تقل عن ســـنة وإلا فإن هذا النص يشكل تراجعاً عن الضـمانات المقررة في المادة (51) من قانون الإجراءات الجزائية الواردة بهذا الخصوص.[179]

وقد أكد على هذا الأمر المقرر الخاص المعني بحرية الرأي والتعبير في تقريره المقدم إلى مجلس حقوق الإنسان في العام 2017 حيث أكد على ضرورة الحصول على إذن من "السلطة القضائية" للمراقبة على المحادثات الســلكية واللاســلكية في الفقرة (19) من التقرير ، و الذي يســتوجب أن تقدم الجهات المعنية بإنفاذ القانون طلبات الكشـــف عن التســـجيلات الهاتفية والبيانات المتعلقة بتحقيقات جنائية للقضاء للموافقة عليها.[180]

كما أكدت على ذلك أيضـاً المبادىء الدولية لتطبيق حقوق الإنســان فيما يتعلق بمراقبة الاتصــالات لعام ،2014 إذ تسعى هذه المبادئ إلى بيان كيفية انطباق قوانين حقوق الإنسان الدولية على البيئة الرّقمية المعاصــرة، خاصــةً بالزيادة في تقنيات وأســاليب مراقبة الاتصــالات و التطور الحاصــل

---

[178] عمار جاموس ، مرجع سابق ، ص 41

[179] عصام عابدين، ملاحظات مؤسسة الحق على مشروع قرار بقانون المعدل للجرائم الالكترونية لسنة 2018، متاح على https://www.alhaq.org/ar/advocacy/2291.html

[180] واقع الخصوصية وحماية البيانات الرقمية في فلسطين، مرجع سابق .

فيها،و هذه المبادئ يمكن أن تكون إطارًا لمجموعات المجتمع المدني ولصـــناعة الاتّصـــالات و للحكومات وغيرها لتقييم اتفاق تشريعات المراقبة الحالية أو المقترحة مع حقوق الإنسان.[181]

فقد شددت على أن القرارات المتعلقة بمراقبة الاتصالات يجب ان تضطلع بها "سلطة قضائية كفؤة ونزيهة ومستقلة ويجب أن تكون منفصلة ومستقلة عن الجهات التي تضطلع بمراقبة الاتصالات" ، كما وينبغي التقيد بالمبادىء الدولية المذكورة من حيث وجوب "إخطار المستخدم" بالأمر القضائي الصـــادر بمراقبة اتصـــالاته، وذلك لضـــمان حقه في الطعن القضـــائي عليه، حيث أكدت المبادئ المذكورة على أن الإخطار القضائي للمستخدم لا ينبغي تأخيره إلاّ إذا كان الإخطار من شأنه إفشال الغرض من المراقبة أو أن يؤدي إلى خطر حال وشـــيك على حياة إنســـان، وفي جميع الأحوال ينبغي "إخطار المستخدم" بأنه قد خضع للمراقبة فور زوال الخطر وعلى النحو الذي تحدده الجهة القضـــائية المختصـــة، كما وينبغي على الحكومة، والشـــركات المزودة لخدمات الانترنت، وفقاً للمبادئ المذكورة، أن تنشـر قوائم دورية تتضـمن عدد طلبات المراقبة التي جرى تنفيذها، والجهة التي طلبت المراقبة، والطلبات التي جرى الموافقة عليها أو رفضها، وبيان الأسباب.[182]

وفي نصـوص المواد( 33 ) و( 34 ) من القرار بقانون ، والتي تمنح الصـلاحية للنيابة العامة أو من تنتدبه من مأموري الضـبط القضـائي، ودون أمر من المحكمة المختصـة، بتفتيش الأشـخاص والأماكن ووسائل تكنولوجيا المعلومات ذات الصلة بالجريمة وضبط الأجهزة والأدوات والبيانات والمعلومات الإلكترونية والتحفظ على كامل نظام المعلومات أو أي وسـيلة من وسـائل تكنولوجيا المعلومات من شـــأنها أن تســـاعد على كشـــف الحقيقة، ودون حضـــور المتهم أو حائز الأجهزة لإجراءات التفتيش والضـــبط، ودون تحديد لمدة أمر التفتيش ، وهذا يخل من ضـــمانات المتهم في مرحلة التحقيق، إذ ينبغي أن تتم تلك الإجراءات بناء على طلب من النيابة العامة، وقرار من المحكمة المختصـــة، وأن تتم في حضـــور المتهم أو حائز الأجهزة وضـــمان توقيعه على محضـــر التفتيش، وأن يكون القرار الصـــادر عن المحكمة المختصـــة بالتفتيش محدداً بالزمن، وذلك حفاظاً على ضـــمانات المتهم في مرحلة التحقيق الابتدائي، وانســـجاماً مع الاتفاقيات والمعايير الدولية ، وهذا ما أكد عليه المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في تقريره المقدم إلى مجلس حقوق الإنسان في العام 2013 ، أذ أورد في التقرير على أنه "ينبغي على الدول أن تنظر إلى مراقبة الاتصـــالات ووســـائل تكنولوجيا المعلومات كعمل تطفلي بدرجة كبيرة ربما

[181] 13 مبدأ حول تطبيق المعايير الدولية على مراقبة الاتصالات " مقال" ، المنتدى العربي لحكومة لانترنت "سمكس" ، https://smex.org/

[182] عصام عابدين، ملاحظات مؤسسة الحق على مشروع قرار بقانون المعدل للجرائم الالكترونية لسنة 2018 ، مرجع سابق.

يتعارض مع الحق في حرية التعبير والحق في الخصـــوصـــية ويهدد دعائم المجتمع الديمقراطي، ويجب على التشريعات أن تنص على وجوب ألا تقوم الدولة بالمراقبة إلا في ظروف إستثنائية جداً، وأن يكون ذلك حصراً تحت إشراف سلطة قضائية مستقلة، ويجب أن يتضمن القانون ضمانات واضـــحة عن طبيعة التدابير الممكنة ونطاقها ومدتها الزمنية والأســـس اللازمة للأمر بها ونوع الانتصاف الذي تتضمنه التشريعات الوطنية" ، و قد أكدت على ذلك أيضاً المبادىء الدولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات 2014 ، أذ نص على أن القرارات المتعلقة بمراقبة الاتصـالات يجب أن تضـطلع بها سـلطة قضـائية كفؤة نزيهة ومسـتقلة منفصـلة عن الجهات التي تضـــطلع بمراقبة الاتصـــالات، علماً بأن تفتيش وســـائل تكنولوجيا المعلومات يندرج في تعريف "مراقبة الاتصالات" بموجب تلك المبادىء الدولية.[183]

ترى الباحثة أن القرار بقانون الجرائم الالكترونية المعدل هو خطوة إيجابية ويحمل في طياته نقاط إيجابية ، لكن و بالرغم من تطرق القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية للحق في الخصـــوصـــية وعلى وجه التحديد في المادة (22) منه إلا أن ذلك لا يعد ســـوا حظراً بالمفهوم الواســـع والعام لاختراق الخصـــوصـــية الرقمية ، ولا يزال بحاجة إلى إجراء تعديلات لتنسجم وتتوازن مع حماية الحق في الخصوصية والتطرق بشكل كامل ولكافة الجوانب المتعلقة بهذا الحق ، وأن يعزز الحريات الأساسية بما يتوافق مع القانون الأساسي والمعايير الدولية ، ومع التزامات فلسطين على الصعيد الدولي.

**- مسودة قرار بقانون حماية البيانات الشخصية الفلسطيني لسنة 2016**

منذ العام 2016 شـــكل مجلس الوزراء لجنة للعمل على إعداد مســـودة قانون لحماية البيانات الشـــخصـــية ، وتم عرضـــها للمرة الثالثة في 15 حزيران 2022 بالقراءة الثالثة على الوزارات المتخصصة للمراجعة وإبداء الملاحظات ، وقد تطرقت مسودة القرار بقانون للنواحي الإجرائية ثم الموضوعية لحماية البيانات الشخصية ضمن تسعاً وثلاثين مادة موزعة على ستة فصول ؛ وتشتمل هذه الفصول على أحكام وتعاريف عامة ، حول معالجة البيانات الشخصية وتبادل ونقل البيانات الشخصية وصولاً إلى العقوبات والأحكام الختامية ، وتعتبر مسودة هذه القانون خطوة إيجابية تجاه تعزيز الحق في الخصوصية الرقمية للمواطن الفلسطيني ، إلا أنه يتضمن العديد من الملاحظات في ما يتعلق بموائمة هذا القرار مع المعايير الدولية،[184]ومن أهمها أن القانون لم

---

[183] عصام عابدين، ملاحظات مؤسسة الحق على مشروع قرار بقانون المعدل للجرائم الالكترونية لسنة 2018، مرجع سابق متاح على https://www.alhaq.org/ar/advocacy/2291.html

[184] الدليل الإجرائي لحماية البيانات الشخصية الفلسطينية في الفضاء الرقمي ، إصدار المركز العربي لتطوير الإعلام الاجتماعي – حملة - ، فلسطين ، 2023 ، ص 9

يوضح مفهوم البيانات الشخصية بدقة ، ولم يحدد المبادئ الأساسية التي تتعلق بجميع العمليات التي تخضع لها البيانات الشخصية في مواجهة كل من له علاقة بها كالمستخدم صاحب البيانات ، والجهة المتحكمة في هذه البيانات ، وأية جهات أخرى قد تعالج هذه البيانات أو تشاركها مع جهةٍ أخرى ، فالمبادئ الدولية ضمن اللائحة الاوربية لحماية البيانات التي ذكرت من خلال الفصل الثالث من هذه الدراسة هي مبادئ جوهرية في رسم الإطار القانوني لمعالجة البيانات الشخصية وتحديد الإجراءات المتعلقة بأمن هذه البيانات وشروط نقلها وتداولها ، وهذه البيانات هي، الشرعية والأنصاف ، تحديد الغرض، مبدأ الحد الأدنى للبيانات، الدقة، تحديد المدد القانونية ، مراعاة حقوق أصحاب البيانات ، النزاهة ، وسرية المعلومات والملاءمة ،[185]وبمراجعة مسودة القرار بقانون حماية البيانات الشخصية فإنه يتضح بأنه تم تضمين المبادئ المذكورة بشكل عام ، دون تركيز على كل مبدأ بشكل خاص ومفصل وضمن مفهوم واسع ، يقتصر على عملية جميع البيانات ومعالجتها ، دون إبداء الاهتمام بالعمليات الأخرى كعملية جمع البيانات الشخصية ونقلها والمشاركة لها ، كما اهتم القرار بالمشروعية ، وأهمية تحديد الغرض من معالجة البيانات ومدتها ، وبضرورة موافقة أصحاب البيانات على المعالجة ، والاعتراض على ما تم معالجته من البيانات، كما أتاحت إمكانية المراجعة لكن ضمن شروط محددة ، لكن فيما يتعلق بالعناية بدقة البيانات بإنها لم تعط العناية الكافية لاهميتها وإمكانية حذفها ،وما يتعلق بحقزق أصحاب هذه البيانات ، الأمر الذي يعرض أصحاب هذه البيانات وحقوقهم للخطر.[186]

وبالتدقيق في المواد المتعلقة بحقوق المستخدمين أصحاب البيانات ، فإن قوانين حماية البيانات الشخصية يجب أن تنص على حقوق المستخدمين أصحاب البيانات الشخصية ، بشكل واضح وصريح وممفهوم، وهذه الحقوق تهدف إلى ضمان حماية بيانات المستخدمين والتحكم بشفافية كاملة ، وتوضخ كيفية التعامل مع بيانات المستخدمين ومعالجتها والكيفية التي تخضع لها، وتقديم وسائل الحماية في حال تم التعامل مع هذه البيانات بشكل غير قانوني ، وهذا مالم ينص عليه مسودة القرار بقانون لحماية البيانات الشخصية الفلسطيني ، لذلك من الضروري النص على هذا الحق بالاستناد إلى الاتفاقيات الدوالية كاللائحة الأوروبية لحماية البيانات ، والمعايير الدولية ومبادئ حقوق الإنسان كون أن فلسطين دولة عضو في معظم الاتفاقيات المتعلقة بحقوق الإنسان ، وذلك لضمان حماية الخصوصية ، وضمان عدم انتهاك حقوق الأفراد ، وتعرض البيانات

---

185 اللائحة الأروبية لحماية البيانات الشخصية ، الفصل الخامس https://gdpr-info.eu/

186 كاثرين ،أبو عمشة ، ورقة موقف حول قرار بقانون حماية البيانات الشخصية ،المركز العربي لتطوير الإعلام الاجتماعي – حملة -، فلسطين ، 2021 ، ص 7

الشخصية للمخاطر التي يترتب عليها العديد من التبعات القانونية وخاصة للجهات التي تختفظ بهذه البيانات أو تعالجها .[187]

وبشكل عام فإن مسودة القرار بقانون حماية البيانات الشخصية الفلسطيني ، فأن نصوص القرار نصت بشكل غير كامل وشامل على الحقوق المتعلقة بأصحاب البيانات الشخصية فيما يتعلق بموضوع نقل البيانات ومعالجتها واعتراضها وحذفها ، وحصرت حقوق أصحاب البيانات في نص المادة 25 منه في : " 1- طلب تصحيح بياناته 2- طلب الحصول على نسخة من بياناته " ، كما تطرقت المادة نفسها إلى سلامة البيانات بشكل ضمني ، وحول حق الحصول على البيانات أو ما يعرف بأمر النفاذ ، بالإضافة إلى تناول نصوص المواد الأخرى إلى حق اللجوء إلى السلطات القضائية في حال التعرض للانتهاكات ، واختصاصات الهيئة الوطنية لحماية البيانات الشخصية في متابعة الشكاوى المتعلقة بالانتهاكات الواقعة على الخصوصية الرقمية ، وتؤكد المسودة على الحق في اللجوء للسلطات القضائية ،كما أكد القرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية على ذلك الأمر ، بخصوص انتهاكات الحق في الخصوصية أو البيانات الشخصية ، وأكدت المسودة على الحق في الحصول على تعويض عادل عند الضرر من إجراء أي عملية متعلقة بالبيانات الشخصية ونصت على العقوبات الجزائية التي تقع على الجهات التي تقوم بمخالفة هذ القانون ، دون التأكيد على الحق في المطالبة والحصول على التعويضات في حال ثبوت الضرر .[188]

إن إقرار قانون حماية البيانات الشخصية في فلسطين أمر ضروري وفي غاية الأهمية ، ومعالجته بالاستناد إلى المعايير الدولية والقانون الأساسي ، خاصة مع التزام فلسيطن دولياً بالمعاهدات والاتفاقيات الموقعة عليها منذ عام 2014 ، وإن أهمية ه1ه المسودة المتعلقة بقانون حماية البيانات يجب أن تتصدر لمعالجتها وموائمتها وتسلسل موادها بشكل متوازن مع المعايير والاتفاقيات الدولية [189]، وذلك لأهمية حماية حق الأفراد في الخصوصية عبر الفضاء الرقمي وأهمية حماية حقوق المستخدمين وبياناتهم من أية انتهاكات ، واتباع إجراءات تسهل على المستخدمين فهم حقوقهم والتزاماتهم وما يترتب على سوء استخدامها .

[187] الدليل الإجرائي لحماية البيانات الشخصية في الفضاء الرقمي، مرجع سابق ، ص 9
[188] كاثرين ، أبو عمشة ، المرجع السابق ، ص 12
[189] الدليل الاجرائي لحماية البيانات الشخصية عبر الفضاء الرقمي ، مرجع سابق، ص 13

كما أن إصـدار التشـريعات الفلسـطينية المتعلقة بحماية الخصـوصـية عبر الفضـاء الرقمي هو أمر بات ملزما وضـروريا ، يجب أن يكون شـاملاً وملزما مسـتند للأسـس القانونية ، ويضـمن حقوق المواطن الفلسطيني ، وتوجيه الوعي والحماية والمساءلة واستقلالية لجميع الأطراف .

# الخاتمة

وبعد أن أنهينا هذه الدراســة عن الحماية الجزائية للحق في الخصــوصــية الرقمية في التشــريع الفلسطيني وفي ضوء المعايير الدولية ، وذلك من حيث تعريفها وطبيعتها ، ومحل الحماية القانونية لها ، ومظاهر المســاس بها، وموقف التشـريعات المقارنة ، والحماية الدولية المكرسـة لحماية هذا الحق، وتحليل مدى انســجام و توافق المعايير الدولية مع التشــريعات الداخلية ، فقد توصــلنا إلى النتائج والتوصيات التالية :

**النتائج:**

1. الخصـوصـية الرقمية هي صـورة مسـتحدثة من صـور الحق الخصـوصـية ، نتجت من أثر التطورات التكنولوجية التي يعتمد الأفرد عليها في كافة الجوانب.
2. الحق بالخصوصية من الحقوق اللصيقة بالإنسان ، ومن الحقوق المعنوية التي لا يمكن للأفراد الاستغناء عن حمايتها ، وانتهاك هذا الحق من الأضرار التي تكون بدرجة كبيرة من الجسامة لاتصالها بحرمة الحياة الخاصة.
3. معظم التشــريعات المقارنة لم تقدم الحماية الكافية لهذا الحق وفقاً للقوانين النافذة لديها، ونتيجة لانتهاكات هذا الحق والتطورات في الجريمة الالكترونية وامتدادها فقد تم التوجه إلى تشــريع نصوص عقابية خاصة لحماية هذا الحق ومواكبة التطورات في العالم الرقمي.
4. المشـرع الفلسـطني لم يضـع قانونا يكفل الحماية الجزائية للخصـوصـية الرقمية بشـكل منفصـل، فالقوانين النافذة لا تكفي لوضــع حد لردع انتهاكات الحق في الخصــوصــية الرقمية ، كما أن النصــوص الموجودة ينبغي أن تكون أكثر وضــوحا وتحديدا لحماية هذا الحق وصــلاحيات الجهات والأفراد في تحديد هذه الانتهاكات ، كما أن الفراغ التشــريعي يشــكل خطراً على المنظومة القانونية ككل ، بحكم ما ينشأ من تجاوزات وأضرار تتطلب تدخلا تشريعياً يتناسب مع حجم تنامي هذه الانتهاكات وخاصةً في ظل التطور التقني.

**التوصيات:**

1. نشـر الوعي في المجتمع بأهمية احترام الحق في الخصـوصـية وعدم المسـاس بهذا الحق، وأن التعرض لهذا الحق يجعلهم محلا للعقاب.

2. نشــر التوعية والتثقيف حول الأمن الرقمي وكيفية حماية الأفراد لخصــوصــياتهم من التعرض للانتهاك ، وذلك من خلال إدخال مساقات تدريسية لطلبة الجامعات ، وإجراء البحوث والدراسات المعمقة ومقارنة الواقع مع القوانين العالمية في موضع الخصوصية الرقمية.

3. ان يكون التشـريع الفلسـطيني على درجة من المرونة والوضـوح من حيث التجريم والعقاب ، وأن تكون العقوبات متناسـبة مع الضـرر ، وعدم اسـتخدام مصـطلحات عامة ، بل يجب أن يكون القانون واضحاً ومحدداً ، وتحديد الجرائم التي تقع في إطار انتهاك الخصوصية الرقمية .

4.الالتزام بما ورد في الإعلانات والمواثيق العالمية ، ومواءمة التشــريعات والســياســات العامة والتطبيقات القضائية معها ومع قوانين حماية الخصوصية وحماية البيانات في العالم.

5. العمل على إيجاد جسـم رقابي أو جهة مسـتقلة معنية بمتابعة ملفات الخصـوصـية والانتهاكات الواقعة على هذا الحق ، ووضع آليات رقابة فعالة لضمان حماية واحترام هذا الحق.

6. إقرار قانون منفرد للخصــوصــية وحماية البيانات لحماية المواطن من الانتهاكات الواقعة عليه من قبل جميع الأطراف.

# قائمة المصادر والمراجع

**أولاً : القرآن الكريم**

**ثانياً: القوانين**

الإعلان العالمي لحقوق الإنسان

القانون الأساسي الفلسطيني المعدل رقم 3 لسنة 2003 م.

قانون الإجراءات الجزائية الفلسطيني رقم 3 لسنة 2001 وتعديلاته.

قرار بقانون رقم 10 لسنة 2018 بشأن الجرائم الالكترونية الفلسطيني .

القانون الأوروبي لحماية البيانات الشخصية "اللائحة العامة لحماية البيانات (GDRR).

قانون العقوبات الأردني رقم 16 لسنة 1960.

الميثاق الوطني الأردني لسنة 1991

قانون الجرائم الالكترونية الأردني رقم 27 لسنة 2015

قانون الاتصالات الأردني رقم 13 لسنة 1995.

قانون مكافحة جرائم تقنية المعلومات المصري رقم 176 لسنة 2018.

قانون حماية البيانات الشخصية المصري رقم 5 لسنة 2020.

قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 .

الدستور المصري لسنة 2012.

مرسـوم رقم 17 الخاص بتنظيم التواصـل على الشـبكة ومكافحة الجريمة المعلوماتية السـوري ، صادر في سنة 2012.

قانون حماية البيانات الشخصية السوري رقم 12 لسنة 2024 .

**ثالثاً: المراجع**

ابن ماجه،ســـنن ابن ماجه، باب حرمة ذم المؤمن وماله، الحديث رقم 3932، تحقيق محمد فؤاد عبد الباقي، دار الفكر، بيروت، ج2 ، ص 1297.

ابن منظور، لسان العرب، دار الأميرية- ط2، ج8، 30 ميلادي.

الأهواني ، ح ، (1978) ، الحق في احترام الحياة الخاصة ، دار النهضة العربية.

سليمان أحمد فضل ، أ، (2007)، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، ط1، دار النهضة العربية.

محمود ، عبد الرحمن ،م ،(1994)، نطاق الحق في الحياة الخاصة ، دار النهضة العربية ، مصر

كريم ، ع ، (2013)، الخصـوصـية الرقمية بين الانتهاك والغياب التشـريعي، مركز دعم لتقنية المعلومات ،القاهرة، ص2.

إبراهيم شمس الدين ، أ ، (2005) ، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات ، دار النهضة العربية ، مصر.

تمام ،أ، (2000) ، الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية ، مصر.

يوليوس، أ ، ( 2009) ، الحماية القانونية للحياة الشـــخصـــية في مجال المعلوماتية ، ط1 ، منشورات الحلبي الحقوقية ، لبنان.

المومني ، ن، (2008) ، الجرائم المعلوماتية ، دار الثقافة ، عمان.

ياسين، ا، (2008) ،المعلوماتية وحضارة العولمة ، ط2، دار النهضة ، مصر.

عطية، م، (1997)، الحق في الحرية الشخصية، المجلة الجنائية ، مصر.

عبد الستار ، ف، (1986) ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية، مصر.

الراعي ، أ ، (2009) ،حق الحصول على المعلومات في التشريع الأردني ، مركز الأردن الجديد للدراسات.

حسبو ،ع، (2000)، حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية، عمان.

الشـــوابكة، م، (2007)، جرائم الحاســـوب والانترنت الجريمة المعلوماتية، ط1 ، دار الثقافة ، عمان.

سرور،أ، الحق في الحياة الخاصة ، مجلة القانون والاقتصاد ، القاهرة.

حجازي ،ع، (2011)، الجرائم المســـتحدثة في نطاق تكنولوجيا الاتصـــالات الحديثة، المركز القومي للاصدارات القانونية ، عمان.

عيســـى، ط ،(2001) ، التنظيم القانوني لشـــبكة الانترنت، دراســـة مقارنة في ضـــوء القوانين الوضعية والاتفاقيات الدولية، منشورات الحلبي الحقوقية ، لبنان.

يوســـف ،أ،(2008)، الجرائم المعلوماتية عبر شـــبكة الانترنت، دار المطبوعات الجامعية ، الإسكندرية.

الفقي،ع، (2006) الجرائم المعلوماتية ، جرائم الحاســـب الآلي والانترنت في مصـــر والدول العربية، المكتب الجامعي الحديث، الإسكندرية.

الزعبي ،ج، محمد ، أ، (2013) ،جرائم تقنية نظم المعلومات الالكترونية ، ط1 ، الإصـــدار الرابع، دار الثقافة ، عمان .

الألفي،م، (2010)، الحماية القانونية لقواعد البيانات في نظم المعلومات ، أعمال وندوات " مكافحة الجريمة عبر الانترنت"، المنظمة العربية للتنمية الإدارية .

الراجحي ، ص،(2004)، حقوق الإنسان وحرياته في الشريعة الإسلامية والقانون الوضعي ، مكتبة العبيكان ، المملكة العربية السعودية.

رابعاً: الأبحاث والرسائل العلمية

عودة ، ي،(2017)، الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة في التشريع العراقي { دراسة مقارنة ، مجلة الحقوق ، الجامعة المستنصرية،} بغداد .

فقيه، ج ،(2017)، حماية البيانات الشخصية في الإعلام الرقمي ، {دراسة مقارنة، جامعة العربي بن المهيدي} ، الجزائر.

مقدر ، ن، بلعسل ، ي،(2021)، الحق في الخصوصية الرقمية، {دراسة ، جامعة يحيى فارس}، الجزائر.

مباركية، م،(2018) ، الحماية الجنائية للحق في الخصـــوصـــية الرقمية في القانون الجزائري، {دراسة مقارنة، جامعة الأمير عبد القادر للعلوم الإسلامية}، الجزائر.

اللامي ، ب، (2017) ، جريمة انتهاك الخصـــوصـــية عبر الوســـائل الالكترونية في التشـــريع الأردني،{ رسالة ماجستير ، جامعة الشرق الأوسط }.الأردن.

سـليم جلاد، س ، (2013) ، الحق في الخصـوصـية بين الضـمانات والضـوابط في التشـريع الجزائري،{ رسالة ماجستير، جامعة وهران }. الجزائر.

عرب ، ي، (2001) ، الخصـــوصـــية وأمن المعلومات في الأعمال اللاســلكية بواســطة الهاتف الخلوي، ورقة عمل مقدمة إلى منتدى العمل الالكتروني بواسطة الهاتف الخلوي ،اتحاد المصارف العربية ، الأردن .

الشيخ يوسف، ي، (1996) ، حماية الحياة الخاصة في القانون الجنائي المقارن،{ رسالة دكتوراه، جامعة القاهرة} . دار الثقافة للنشروالتوزيع ، الأردن، ص 200.

قوتال ، ي، ( 2018) ، حق الخصـــوصـــية الالكترونية بين التقييد والإطلاق ،{ بحث}، جامعة عباس الغرور، خنشلة، الجزائر ، ص57.

السيد راشد، ط ، (2016) ، مدى حجية رسائل التواصل الاجتماعي في الإثبات {دراسة تحليلية مقارنة}. مجلة العلوم القانونية، جامعة عين شمس.

عصام،أ، (2013) ، تأثير مواقع التواصل الاجتماعي على خصوصية الفرد الجزائري، {رسالة ماجستير، كلية العلوم الإنسانية ، جامعة المسيلة } .الجزائر.

الموسوي، م، (2013) ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها{بحث}، مجلة كلية بغداد للعلوم الأقتصادية.

المهدي، ع، (1987)، الجوانب الإجرائية لحماية الحق في الحياة الخاصة{بحث} . مؤتمر الحق في الحياة الخاصة ، جامعة الإسكندرية

أبو حجيلة، م، (2007) ، الحماية الجزائية للمعلومات الشخصية للأفراد في مواجهة أخطار بنوك المعلومات ، {رسالة ماجستير ، جامعة آل البيت}.الأردن.

تافارا، أ، (2020) ، مقال بعنوان أهمية حماية الخصوصية في عصر البيانات الرقمي، مدونات البنك الدولي .

ماروك، ن، (2003) ،مقال بعنوان الحق في الخصوصية ، مجلة النائب، العدد 20، الجزائر.

كليب ، آ، (2021) ،قانون حماية البيانات المصري في ضوء المعايير الدولية ، مؤسسة حرية الفكر والتعبير ، القاهرة .

آمنة الصيادي،آ، (2021) ، البيانات الشخصية:ما مدى أهمية حمايتها وهل من تشريع؟، منظمة اكسس ناو.

الانتهاكات الرقمية للفلسطينيين ، دراسة ، من قبل مركز صدى الإعلامي ، رام الله ، فلسطين ، 2024.

إبراهيم شمس الدين ،إ، (2005) ، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات ، دار النهضة العربية، مصر .

الصغير،ج،(2000) ، الانترنت والقانون الجنائي، دار النهضة العربية ، مصر .

تمام ، ح، (2000) ، الجرائم الناشئة عن استخدام الحاسب الآلي ، دار النهضة العربية، مصر.

رزق ،ه ، (2021) ، مفهوم الذكاء الاصطناعي ، { بحث}، مجلة دراسات في التعليم الجامعي، تونس.

بومديان ، م ،(2021) ، الذكاء الاصطناعي تحد جديد للقانون ،{ بحث} ، مجلة مسارات للأبحاث والدراسات القانونية، المغرب .

بن قارة ،ع ، (2006) ، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية{ بحث} ، مجلة البحوث القانونية والسياسية ، تونس.

دهشان ، ي ، (2020) ، المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، مصر.

إبراهيم ، م، (2022) ، التنظيم التشريعي لتطبيقات الذكاء الاصطناعي ، مجلة البحوث القانونية والاقتصادية، الإمارات.

براك ،أ، (2023) ، إشكالية المسؤولية الجزائية لتقنيات الذكاء الاصطناعي ، مركز البحوث القانونية، العراق

عميمر ، ع ، (2018) ، الحماية الجنائية للحق في الحياة الخاصـــة في البيئة الرقمية، {رســـالة ماجستير، جامعة الحسن الأول }، المغرب .

صقر، ي، (2006) ، حماية حقوق الشخصية في إطار المسؤولية التقصيرية " دراسة مقارنة" ،{ رسالة دكتوراه ، جامعة الأزهر}.فلسطين.

ميســـروب، س ،(2017) حماية الحق في ســـرية المكالمات الهاتفية والالكترونية{بحث} مجلة بحوث مستقبلية، جامعة كركوك ، العراق.

صـــالح، ر،(1993)، الحق في الحياة الخاصـــة وضـــماناته في مواجهة اســـتخدامات الكمبيوتر، {رسالة ماجستير ، جامعة بغداد } . العراق .

مطر، م، صالحة، ن ،(2020) ، تحديات الحقوق الرقمية في فلسطين، المركز الفلسطيني للتنمية الحريات الإعلامية " مدى.

سـمودي، ر،(2017) ، الموقف المعاصـر للقانون الدولي العام من الحق في الخصـوصـية في العصر الرقمي ، مجلة الجامعة العربية الأمريكية للبحوث، (3) 2 ، 2017.

غزيل،ع، (2022)، الحماية الدولية للحق في الخصوصية في العصر الرقمي ، {رسالة ماجستير، جامعة غليزان} . الجزائر.

شـقير، ي، (2012)، مدى توافق قانون الحصـول على المعلومات في الأردن مع المعايير الدولية [ رسالة ماجستير- جامعة الشرق الأوسط }. الأردن.

الهنـدي، م، (2018) ، نفـاذ قـانون الجرائم الالكتروني"المجتمع المـدني وانكفـاء الـدور،المركز الفلسطيني لأبحاث السياسات والدراسات الاستراتيجية "مسارات".

عـابـدين،ع، (2018) ، ولايـة المقرر الخـاص المعني بتعزيز وحمـايـة الحق في حريـة الرأي والتعبير، مؤسسة الحق.

فطافطة ، م، سـمارو ، د، (2021) ، حماية البيانات في منطقة الشـرق الأوسـط وجنوب افريقيا، منظمة أكسس ناو.

جاموس،ع، (2022) ،الحق في الخصـــوصـــية بين المعايير الدولية والواقع الفلســـطيني، الهيئة المستقلة لحقوق الإنسان.

أبو عرقوب،ع، (2021)، واقع الخصـــوصـــية وحماية البيانات الرقمية في فلســـطين ، المركز العربي لتطوير الإعلام الاجتماعي، "حملة".

قطاع الاتصـــالات وتكنولوجيا المعلومات والحقوق الرقمية الفلســـطينية "ورقة حقائق"،(2021)، مركز الميزان لحقوق الإنسان.

على فلسطين إصلاح قانون الجرائم الالكترونية التقييدي 2017 هيومن رايتس ووتش.

التشـــريع الالكتروني ومدى مراعاة الحقوق والحريات العامة " ورقة موقف " ،(2017) ، مركز الميزان لحقوق الإنسان ، فلسطين.

الانتهاكات الرقمية للفلسطينيين ، مركز صدى الإعلامي "دراسة "،(2024) ، فلسطين .

13 مبدأ حول تطبيق المعايير الدولية على مراقبة الاتصـــــالات " مقال" ، (2016) ،المنتدى العربي لحكومة الانترنت "سمكس" .

الدليل الإجرائي لحماية البيانات الشـخصـية الفلسـطينية في الفضـاء الرقمي ، (2023)، المركز العربي لتطوير الإعلام الاجتماعي – حملة - ، فلسطين.

كاثرين ، أبو عمشـــة ، ورقة موقف حول قرار بقانون حماية البيانات الشـــخصـــية ، (2021) ، المركز العربي لتطوير الإعلام الاجتماعي – حملة - ، فلسطين.

**خامساً : المواثيق الدولية**

الاتفاقية الأمريكية لحقوق الأنسان لسنة 1969.

الميثاق العربي لحقوق الإنسان لسنة 2004.

العهد الدولي الخاص بالحقوق المدنية والســـياســـية ، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 2200(د-21) ،المؤرخ في 16 ديسمبر 1966.

التقرير التفسيري لاتفاقية بوادبست لمكافحة الجريمة الالكترونية ، مجلس أوروبا لحقوق الإنسان .

مبادئ ســـيراكوزا المتعلقة بأحكام التقييد و عدم التقيد الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية.

التقرير السنوي للمفوضية السامية للأمم المتحدة لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي،2014.

www.ohchr.org

*الوثائق الرســـمية للجمعية العامة، الدورة الثالثة والأربعون، الملحق رقم 40* (A/43/40)، المرفق السادس.

www.ohchr.org

التعليق العام رقم 31 (80) ،اللجنة المعنية بحقوق الإنســان، الدورة الثامنة عشــرة ،العهد الدولي الخاص بالحقوق المدنية والسياسية . CCPR/C/21/Rev.1/Add. 2004

www.ohchr.org

اللجنة المعنية بحقوق الإنســـان (2013) ، التعليق العام رقم 35 على المادة 9 من العهد الدولي الخاص بالحقوق المدنية والسياسية المعنية بالحق في الحرية والأمان الشخصي.

**سادساً: القرارات القضائية**

محكمة التمييز الأردنية ، القرار رقم 2003/818 الصادر في 3 حزيران 2003.

محكمة بداية عمان ، القرار رقم 2009/550 بتاريخ 28 أيار 2009.

## Abstract

This groundbreaking study delves into the complex world of digital privacy, shedding light on the efficacy of international laws in safeguarding our personal data. Through a comprehensive and thorough analysis of diverse texts and comparative legislation, this research seeks to unveil the reality of privacy protection in the digital age, providing a solid foundation for further discussion and analysis.

This comprehensive study delved into the historical origin of privacy and meticulously tracked its evolution in response to the emergence of modern technology and communication. It scrutinized the definition of personal data and emphasized the necessity of safeguarding it from unauthorized access and exploitation across various sectors. Furthermore, the study focused on empowering users by addressing violations of their digital privacy rights and explored legal measures designed to protect digital privacy. It also meticulously reviewed guidelines and international standards, emphasizing the critical need to align them with national legislation. This alignment is not only a key recommendation of the study but also has the potential to significantly impact the work of legal professionals, policymakers, researchers, and advocates for digital privacy.

The comprehensive study has unequivocally shown that safeguarding the right to privacy in the digital era is a collective responsibility that involves multiple stakeholders. International laws have laid down clear guidelines for ensuring the protection of this fundamental right and have mandated nations to enforce penalties for any privacy breaches. Additionally, it has been emphasized that the right to privacy is the cornerstone for realizing other rights and liberties. Therefore, the Palestinian legislator must take concrete steps to not only safeguard individual privacy but also to enact dedicated

legislation to safeguard digital data in Palestine. This is not just a matter of compliance but a crucial step towards upholding the rights of every individual.

Keywords: Right to privacy, digital privacy, personal data, artificial intelligence, international standards, criminal protection of the right to digital privacy.