مجلة ننار للعلوم الإنسانية والاجتماعية
جامعة الحلة
ISSN-L: 3005- ISSN-P: 3005-8236
DOI Prefix: 10.64002

# حدود الحماية الدولية للحق في الخصوصية المعلوماتية

**م.د. زيد محمد كاظم الحسيني**

[1] كلية الامام الكاظم (ع) اقسام بابل، العراق.

*الايميل: bqndyl48@gmail.com

تاريخ استلام : 2026/3/28 تاريخ القبول: 2026/5/10 تاريخ نشر :2026/06/20

## الملخص

يشهد العالم اليوم تطوراً كبيراً في الثورة الرقمية للتكنلوجيا والاتصالات، أدى ذلك الى بروز مفاهيم جديدة تتطلب الحماية القانونية ومن ذلك مصطلح الخصوصية المعلوماتية، التي تعد جزء لا يتجزأ من الحق في الحياة الخاصة، والحق في الحياة الخاصة احد اهم الحقوق التي تمنح للإنسان، وهذا ما أكدته الصكوك الدولية وعلى رأسها الاعلان العالمي لحقوق الانسان الصادر من الجمعية العامة للأمم المتحدة ١٩٤٨، فضلاً عن نص العهد الدولي للحقوق المدنية والسياسية لعام ١٩٦٦ في نص مطابق لما جاء به من الاعلان العالمي لحقوق الانسان.

إضافة الى العديد من الاتفاقيات الأخرى والاعلانات والمؤتمرات على الصعيدين الدولي والاقليمي، وفي ظل التطور الرقمي تجلت صور عدة للحق في الخصوصية الرقمية في مظهر مغاير عما كانت عليه عناصر الحق في الحياة الخاصة التي كادت تقتصر على حرمة المسكن)، فظهرت خصوصية البيانات الشخصية والبيانات المالية الرقمية الصحية وأيضاً سرية الاتصالات والمراسلات الالكترونية وغيرها، لذا كان الغرض من هذه الدراسة هو تسليط الضوء على الحماية القانونية لهذا الحق في أطر الاتفاقيات الدولية والتشريعات العراقية، وذلك بسبب ما يتعرض له هذا الحق من انتهاك واضح ومباشر، اذ على الرغم مما نصت عليه الصكوك الدولية لحماية الحق في الحياة الخاصة، الا أن نلاحظ القصور الواضح في بعض التشريعات لحماية الحق في الخصوصية الرقمية بشكل محدد، اذ أن هناك فراغ تشريعي واضح في التشريعات الوطنية فباتت النصوص التقليدية التي تحمي الحق في الحياة الخاصة بصورة عامة لا تتناسب مع هذه الانتهاك الالكترونية التي يتعرض لها الحق في الخصوصية الرقمية، ورغم ذلك كان للقضاء دور بارز في ضمان حماية هذا الحق، وفي النهاية نلحظ أن هذا الحق ليس حق مطلق بل ترد عليه قيود تستهدف حماية مصالح الافراد والمجتمع، سواء كانت هذه القيود دستورية ام جنائية، اذ قيدت أغلب التشريعات عدم التعسف في استعمال الحق وانتهاك خصوصية الافراد الا بأمر قضائي.

**الكلمات المفتاحية:**

**الحماية القانونية، الخصوصية الرقمية، التشريعات الوطنية.**



Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)

https://doi.org/10.64002/63tzss98

# Limits of International Protection of the Right to Information Privacy

**Asst. Dr. Zaid Mohammed Kazim Al-Husseini**

[1] Imam Al-Kadhim College (PBUH) – Babylon Departments, Iraq.

*Corresponding author: bqndyl48@gmail.com

**Received date: 28/03/2026** **Accepted date: 15/05/2026** **Published date: 20/06/2026**

## Abstract

The world today is witnessing rapid development in the digital revolution of technology and communications. This development has led to the emergence of new concepts that require legal protection, among which is the concept of digital privacy. Digital privacy is considered an integral part of the right to private life, which is one of the most fundamental rights granted to individuals. This has been affirmed by international instruments, most notably the United Nations's Universal Declaration of Human Rights issued by the General Assembly in 1948, as well as the International Covenant on Civil and Political Rights of 1966, which includes provisions consistent with those stated in the Universal Declaration of Human Rights.

In addition to numerous of other agreements, declarations, and conferences at both the international and regional levels have addressed this matter. With the advancement of digital technology, various forms of the right to digital privacy have emerged in ways that differ from the traditional elements of the right to private life, which were previously almost limited to the inviolability of the home. Consequently, new aspects have appeared, including the privacy of personal data, financial and digital health data, as well as the confidentiality of electronic communications and correspondence, among others.

Accordingly, the aim of this study is to shed light on the legal protection of this right within the framework of international agreements and Iraqi legislation. This is particularly important due to the clear and direct violations to which this right is exposed. Despite the provisions of international instruments protecting the right to private life, there remains a noticeable deficiency in certain legislations regarding the specific protection of digital privacy. There is a clear legislative gap within national legal systems, as traditional legal provisions designed to protect the right to private life in general are no longer sufficient to address the electronic violations affecting digital privacy.

Nevertheless, the judiciary has played a significant role in ensuring the protection of this right. Finally, it should be noted that this right is not absolute; rather, it is subject to certain restrictions intended to safeguard the interests of both individuals and society. These restrictions may be constitutional or criminal in nature. Most legislations, therefore, limit the abuse of this right and prohibit violations of individuals' privacy except by judicial authorization.

**Keywords:**

**Legal protection, digital privacy, national legislation.**



Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)

https://doi.org/10.64002/63tzss98

## المقدمة

### اولاً: موضوع الدراسة

تُعدّ الخصوصية المعلوماتية من أبرز الحقوق التي اكتسبت أهمية متزايدة في ظل التحولات الرقمية المتسارعة التي يشهدها العالم المعاصر، فقد أدى التطور التكنولوجي الهائل، وانتشار شبكة الإنترنت، وتنامي استخدام وسائل التواصل الاجتماعي، إلى تضخم حجم البيانات الشخصية المتداولة يوميًا، ما جعل حماية هذا الحق تحديًا قانونيًا وأخلاقيًا يتجاوز الحدود الوطنية، وانطلاقًا من الاعتراف الدولي بالحق في الخصوصية ضمن الأمم المتحدة، أصبح من الضروري إعادة قراءة هذه النصوص في ضوء البيئة الرقمية الحديثة وما أفرزته من إشكاليات غير مسبوقة.

لقد أفرزت الثورة الرقمية واقعًا جديدًا أصبحت فيه البيانات الشخصية موردًا اقتصاديًا واستراتيجيًا، تتنافس عليه الدول والشركات الكبرى، الأمر الذي زاد من احتمالات انتهاك الخصوصية عبر المراقبة الرقمية، والتجسس الإلكتروني، وتحليل البيانات الضخمة، والذكاء الاصطناعي، كما أن الطبيعة العابرة للحدود لتدفق المعلومات عبر الفضاء السيبراني تطرح إشكالات تتعلق بالاختصاص القضائي وتعارض القوانين، مما يضعف فعالية الحماية الدولية التقليدية المبنية على سيادة الدولة، وتزداد حدة هذه التحديات في ظل غياب إطار قانوني دولي موحد ومُلزم ينظم معالجة البيانات الشخصية على المستوى العالمي.

إضافة إلى ذلك، يثير التوازن بين متطلبات الأمن القومي ومكافحة الإرهاب من جهة، وحماية الخصوصية المعلوماتية من جهة أخرى، جدلًا واسعًا في الفقه القانوني والسياسات العامة وعليه، فإن دراسة التحديات او القيود المعاصرة للحماية الدولية للحق في الخصوصية المعلوماتية تكتسب أهمية بالغة، إذ تتطلب تحليلًا نقديًا للمنظومة القانونية الدولية الراهنة، وتقييم مدى كفايتها في مواجهة المخاطر الرقمية، واستشراف سبل تطوير آليات أكثر فاعلية تضمن حماية هذا الحق في عالم تتداخل فيه الحدود المادية مع الفضاءات الافتراضية، ومن هنا تنطلق أهمية هذا البحث في محاولة تسليط الضوء على أبرز الإشكالات القانونية والعملية التي تعترض الحماية الدولية للخصوصية المعلوماتية، واقتراح رؤى تسهم في تعزيز ضماناتها في السياق الرقمي المعاصر.

### ثانياً: اهمية الدراسة

تكمن اهمية الموضوع في ان الخصوصية المعلوماتية من المواضيع الحديثة التي تتطلب المزيد من البحث في ظل التطور التكنولوجي المعاصر، والذي قابله انتهاك وتدخل في الخصوصية المعلوماتية للافراد، حيث نتج عنه تحديات وقيود كثيرة فرضت واقعاً قانونياً صعباً في توفير الحماية الكافية للخصوصية المعلوماتية.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

### ثالثاً: هدف الدراسة

ان الهدف من الدراسة هو بيان الحماية الدولية للحق في الخصوصية المعلوماتية وتحديد التحديات القيود التي تعرقل تلك الحماية على الأصعدة كافة، وتنبثق منه مجموعة اهداف تتمثل بالآتي:

1. بيان موقف المشرع الوطني في توفير الحماية وماهية القيود التي فرضت في توفير الحماية.
2. محاولة تحديد القيود الجنائية المفروضة على ضمان الحق في الخصوصية وتشخيص القيود التي تقف عائقاً في طريق الحماية الجنائية والدولية، وبحث إمكانية تطوير وسائل الحماية..
3. بيان الجهود الدولية والاقليمية التي بذلت من اجل حماية الحق في الخصوصية المعلوماتية.
4. بيان مدى تعارض الحق في الخصوصية المعلوماتية مع حقوق الانسان الاخرى.
5. بيان الموقف القانوني والاجراءات القضائية المعمول بها اثناء انتهاك الحق.

### رابعاً: اشكالية الدراسة

تتعاظم اشكالية البحث في اختراق الخصوصية المعلوماتية في جميع دول العالم، وما يترتب على هذه الانتهاكات من مشاكل اقتصادية واجتماعية وسياسية تهدد امن المجتمع الدولي بصورة عامة.

- ماهية الحماية الدولية للحق في الخصوصية المعلوماتية؟
- بيان الضمانات الدولية لتعزيز الحماية الدولية؟
- كيف ساهمت التشريعات الوطنية في توفير الحماية؟
- ما هو موقف الامم المتحدة ازاء الانتهاكات الكبيرة لهذا الحق؟
- ما هو موقف القضاء الجنائي الدولي من الحماية؟

### خامساً: منهجية الدراسة

يتم اعتماد المنهج الوصفي والمنهج التحليلي والاستقرائي، من اجل تحليل النصوص القانونية التي وضعت من اجل بحث جرائم التعدي على الحياة الخاصة، كذلك تحليل نصوص الاتفاقيات والمواثيق الدولية، ووصف بعض صور وتطبيقات الانتهاكات الواقعة على الحق في الخصوصية المعلوماتية للافراد، وبيان فعالية تلك النصوص في تحقيق الحماية.

### سادساً: خطة الدراسة

ان الاحاطة بموضوع التحديات او القيود الدولية الخاصة بحماية الحق في الخصوصية المعلوماتية يتطلب دراسة اكاديمية بنوع من الشمولية وهذا يتطلب منا ادراج مقدمة عن الموضوع تتضمن الاهمية والاهداف والاشكالية ومن ثم تقسيم البحث الى ثلاثة مطالب، اذ نبحث في المطلب الأول بيان قيود التعاون الدولية والوطنية واستعراض موقف التشريعات من الحق في الخصوصية، في حين خصصنا المطلب الثاني من البحث لدراسة القيود الجنائية على الحق في الخصوصية المعلوماتية، اما المطلب


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

الثالث خصص لبحث إمكانية تطوير الحماية الدولية، ومن ثم نلحق البحث بخاتمة تتضمن مجموعة من النتائج والمقترحات.

## المطلب الاول

## قيود التعاون الدولية والوطنية

### اولاً: القيود والمعوقات الدولية

ان تحديد الصعوبات التي تواجه التعاون الدولي يعد خطوة اولى حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل حيزاً كبيراً على الحكومات والمختصين والأفراد على حد سواء ولقد أثبت الواقع العملي أن الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة فنتيجة للتطور الكبير والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الإنترنت ومن ثم الذكاء الاصطناعي والانتشار الواسع والسريع لهما أدى إلى ظهور أشكال وأنماط جديدة من الجرائم منها الجرائم المتعلقة بالمعلوماتية التي باتت تشكل خطرا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة لكيان المجتمع[1]، وكذلك شملت الاعتداء على خصوصية الدول والافراد على حد سواء، إلا أنه ثمة صعوبات ومعوقات تقف دون تحقيق التعاون الدولي في هذا المجال نوجز أهمها:

#### 1. عدم وجود نمط موحد للنشاط الإجرامي

بنظرة متأنية للأنظمة القانونية في التشريعات العربية والاجنبية لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت يتضح لنا من خلالها عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمهما، فما يكون محظوراً في نظام يكون مباحاً في اخر، ويمكن ارجاء ذلك لعدة اسباب منها اختلاف البيئة، العادات والتقاليد، الديانة، الثقافة، وبالتالي اختلاف السياسة التشريعية من دولة لأخرى[2].

#### 2. اختلاف النظم القانونية الإجرائية

بسبب تنوع واختلاف النظم القانونية الإجرائية من بلد الى اخر، نجد أن طرق التحري و التحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها، كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم

(1) تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الاجتماعية، بانكوك، 2005، وثيقة رقم203.

(2) عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر، دار الكتب القانونية، القاهرة, 2002، ص102.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

المراقب والعمليات المستترة، وغيرها من الإجراءات، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى وبالتالي فإن الدولة الأولى سوف تشعر بخيبة أمل لعدم قدرة سلطات إنقاذ القانون في الدولة الأخرى على استخدام ما تعتبره هي أنه أداة فعالة، بالإضافة إلى أن السلطات القضائية لدى الدولة الثانية قد لا تسمح باستخدام أي دليل إثبات جرى الحصول عليه بطرق ترى هذه الدولة أنها طرق غير مشروعة حتى وإن كان هذا الدليل تم الحصول عليه بناء على اختصاص قضائي وبشكل مشروع[1].

### 3. عدم وجود قنوات اتصال[2]

ان العمل على التعاون الدولي في مجال مكافحة الجريمة والمجرمين للحصول على المعلومات والبيانات المتعلقة بهم، ولتحقيق هذا الهدف كان لزاما أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات اجنبية من اجل التعاون وجمع المعلومات وبالتالي تعزيز القدرة والخبرة اللازمة في عملية التصدي لجرائم المعلوماتية، الا ان هنالك دولاً قد عملت على اتفاقيات ثنائية ذات طبيعة تعاون مشترك في عمليات التجارة او الصناعة او التجهيزات العسكرية او الدفاع المشترك، وهذا ما يرفع من امكانية الحماية مستقبلاً.

### 4. مشكلة الاختصاص

تعد جرائم الخصوصية المعلوماتية من أكبر الجرائم التي تثار بشأنها مشكلة الاختصاص، يتم ذلك على المستوى الدولي عكس المستوى المحلي الذي حدد الاختصاص حسب أحد المعايير (مكان القبض على المتهم، مكان وقوع الجريمة، محل الاقامة) اما المستوى الدولي وبسبب اختلاف التشريعات والنظم القانونية تظهر هذه المشكلة متمثلة بتنازع القوانين او تنازع الاختصاص كونها من الجرائم العابرة للحدود، فهل تخضع لمبدأ العينية ام الاقليمية.

ايضاً من المعوقات التي تعيق عمل التعاون الدولي مشكلة (التجريم المزدوج)، وكذلك مشكلة (المساعدات القضائية)، ومن ثم مشكلة التدريب التي تتمثل في عدم اهتمام بعض الدول بالتدريب وتطوير القدرات الادارية والمعلوماتية لدى قياداتها، خصوصاً في مجال تكنولوجيا المعلومات والقضايا الالكترونية المستحدثة، بالمقابل نجد ان الجريمة الالكترونية الخاصة بالمعلوماتية قد تطورت بشكل

(1) محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، مركز الدراسات العربية، مصر، 2015، ص112.

(2) عبد الله محمد صالح الشهري، المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، جامعة الملك سعود، الرياض، المملكة العربية السعودية، 2002، ص118.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

هائل، وهذا يتطلب تعزيز قدرات الجهات المعنية بتوفير الحماية في جميع القطاعات، اذ لا يتم ذلك الا من خلال التدريب والتعاون الدولي المشترك.

### ثانياً: القيود والمعوقات الداخلية

يقصد بالقيود الواردة على المساس بالحق في الخصوصية، الحالات التي يمكن فيها الكشف عن الحياة الخاصة إلى العلن، من دون اعتبار الفعل من الناحية القانونية انتهاك للخصوصية، فهو مثل معظم الحقوق يخضع وفقا للظروف معينة، وفي أحوال محددة لبعض القيود والاستثناءات التي تنفي عنه الحماية القانونية، حيث يصبح المساس به مشروعا، و إذا ما أردنا أن نحدد هذه الاعتبارات التي قرر فيها كل من الفقه والقضاء المقارنين إمكانية إزاحة الستار عن الحياة الخاصة للأفراد دون أن يعتبر ذلك انتهاكا لحرمتها، نقول أن هناك اعتبارات عدة خلص إليها كل من الفقه والقضاء في عديد من الدول واعتبارها بمثابة قيود على الحق في الخصوصية وهي كالتالي.

#### 1. الرضا والحق في الخصوصية

ذهب القضاء المعاصر إلى أنه يحظر تنازل الشخص عن حقه في الحياة الخاصة بصفة نهائية، ولكن يجوز أن يكون هذا الحق محلا لاتفاقات تتعلق بممارسته أو تسمح بالتنازل عنه شريطة أن تكون هذه الاتفاقات مشروعة و لا تتعارض مع النظام العام و الآداب العامة، و الرضا الذي يصلح كسب للإباحة يجب أن يكون صادرا عن إرادة حرة وصحيحة و خالية مما يعيبها، وبذلك يملك الشخص الحق في تحديد ما يمكن نشره، وما يجب أن يظل في الكتمان من أمور حياته الخاصة، فالرضا يعني بصفة عامة الموافقة على اتخاذ إجراء معين في مواجهته، فهو بمثابة تعبير عن إرادة الشخص نحو قبول أمر معين، وفي المجال الجنائي يعني اتجاه الإرادة نحو قبول فعل الاعتداء على مصلحة يحميها القانون[1]، و الشروط التي يجب أن يتم النشر طبقا لها هي :

- **أن يصدر الرضا من صاحب المصلحة:** الرضا الذي يبيح المساس بالحياة الخاصة هو ذلك الذي يصدر من صاحب الصفة في إصداره أي صاحب الحق أي صاحب الحق نفسه، فمتى صدرت الموافقة الشخصية منه بالكشف عن الخصوصية كان ذلك مبرر للمساس بالحق.
- **أن يكون الرضا خاصاً ومحدداً:** إن الشخص الذي يقوم باتفاق ما بشأن خصوصياته يكون أباح الاطلاع عليها في إطار الاتفاق الحاصل بينه وبين الناشر، إذ لا ينبغي أن نفهم من رضا الشخص تنازله النهائي عن حقه في الخصوصية فمثلا المجلة التي تتعرض للحياة الخاصة

(1) خلاف بيرو، تطور حماية الحياة الخاصة للعامل، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص تحولات الدولة، كلية الحقوق و العلوم السياسية، جامعة قصدي مرباح ، ورقلة ، 2010 ص 22.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

لأحد الأشخاص بناء على موافقة هذا الأخير في مقابلة صحفية يمنع عليها نشر معلومات لم يدلي بها الشخص أثناء المقابلة ولم يعطي الموافقة على نشرها.

- **أن لا ينطوي الرضا على مخالفة للنظام العام والآداب العامة:** من الشروط التي يجب أن تتوفر في الرضا المقيد للخصوصية هو عدم مخالفته لقواعد العام والآداب العامة السائدة داخل الدولة، في ظل المنظومة القانونية الجزائرية لا يمكن نشر صورة شخص وهو في وضع مخل بالحياء ولو تم ذلك برضاه[1] .

ومن ثم فإن الرضا يبيح التدخل أو التحري في الحياة الخاصة، ويجب التزام من حصل على الرضا بنشر الوقائع التي كانت محلا للرضا فقط، ولا يملك التعرض لوقائع أخرى غير تلك التي تمت الموافقة على نشرها بغض النظر عن أشكال الرضا اذ لم يشترط القانون شكلا معينا لرضا، مادام يمكننا أن نستنتج الإرادة الحقيقية للشخص سواء كان (الرضا الصريح، الرضا الضمني، الرضا المفترض)

### 2. الحق في الإعلام والحق في الخصوصية:

في ضوء ازدياد أهمية الإعلام و السباق المحموم للحصول على الأخبار و خاصة تلك التي تتعلق بالحياة الخاصة بشخصيات سياسية أو فنية أو رياضية، وحتى للأفراد العاديين، وما تهدف إليه بعض وسائل الإعلام من تعقب خصوصيات الأفراد و أسرارهم تدخلاً على الحق في الخصوصية، سعيا وراء مكاسب مادية أو سياسية أو غير ذلك، مما يؤدي إلى انتهاك حرمة الحياة الخاصة، وكشف حجب سريتها، ومن هنا يصطدم الحق في تدفق المعلومات بالحق في حرمة الحياة الخاصة و كلاهما مقيد بما تقتضيه مصلحة المجتمع من الموازنة بين الحق في الخصوصية[2].

فحرية الإعلام هي إحدى صور حرية التعبير التي كفلتها الدساتير والتشريعات الوطنية فلا يمكن التذرع بحق الإعلام للمساس بحق الخصوصية، لاسيما أن كل حق هو نقيض للآخر، أحدهما يحمي حق المجتمع في الإعلام والآخر يحمي حق الشخص في الخصوصية و عدم كشفها للغير دون رضاه، فمن جانب اهتمام الجمهور بمعرفة خصوصيات الشخص المشهور ، لا يكون لمجرد حب الاطلاع الشخصي و إنما دافع المصلحة العامة، حتى تلقى الضوء على حياته خاصة و بالتالي يكون النشر مشروعا بدون إذن، متى كان ذلك تحقيق للمصلحة العامة وبخلافه لا يجوز النشر الا بموافقة صاحب الحق.

(1) محمد بن حيدة، الحق في الخصوصية في التشريع الجزائري (دراسة مقارنة) ، مذكرة لنيل شهادة الماجستير، تخصص حقوق و حريات، قسم العلوم القانونية و الإدارية، كلية الآداب والعلوم الإنسانية، الجامعة الإفريقية العقيد أحمد دراية، 2009، ص129.

(2) بسمة بوكروم وايمان بوفليغة, الحق في الخصوصية في ظل الرقمية، رسالة ماجستير، جامعة محمد الصديق بن يحيى، كلية الحقوق والسياسة، 2019، ص 108.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

### 3. حق الشخص في السرية وحق الجمهور في الاطلاع

لا يتصور أن يكشف الشخص عن جوانبه الخاصة به أمام الجميع، صوره أو بياناته الشخصية، أو انتماءاته أو عرقه، وحتى أموره الخاصة به لكون أن جوهر الحياة الخاصة هي السرية، ولكونها تحفظ جوانب حياته الشخصية ولعل ما زاد في فرص إطلاع الغير على بعض من خصوصيات الشخص هو اتساع مجال هذه الحق في الخصوصية عبر استخدام شبكة الإنترنت في نشر البيانات المتعلقة بالشخص، كحالته الصحية أو العائلية والمالية والفكرية، بحيث يتم تبادل المعلومات ما بين الشبكات والحواسيب بسرعة وسهولة، وعبر المواقع أو البريد الإلكتروني، كما قد يلجأ أحد الأشخاص للتسجيل في أحد المواقع طلباً لعلم أو دراسة أو عمل، وهنا أصبحت خصوصيات الشخص عرضة للاطلاع من قبل الغير، سواء رغب الشخص في ذلك أم لا.

كما قد يلجأ مستهلك الكتروني إلى أحد المواقع التجارية الإلكترونية طلباً لخدمة أو سعياً لجلب منتوج أو سلعة، فتطلب تلك الشركات تعبئة نموذج خاص يحتوي على عدد من البيانات التي يجب ملئها، اسم المستخدم، عنوانه، رقم هاتفه وبريده الالكتروني، ومكان إقامته ودخله الشهري وغيرها، وعليه فتطور تقنية الاتصالات صارت أداة تهدد حياة الشخص وخصوصيته؛ لأن تدفق المعلومات عبر شبكة الانترنت قد سهل مهمة التعرف على الأشخاص أو جعلته قابلاً للتعرف عليه عبر بياناته الشخصية، خاصة إذا كان لا يرغب في نشرها[1]، ولعل هذا ما يبرز تطور آليات حماية هذا الحق كما سنشير لاحقاً.

### 4. حق الشخص في السرية وحق الدولة في الرقابة

تبعاً لهذا المفهوم الجديد للحق في الخصوصية؛ وهو حماية الحق في المعلوماتية، أفرز ذلك أيضاً تغير في خصائص هذا الحق، فلم يعد الأمر سرياً للغاية؛ لأن مجال الاتصالات الإلكترونية أفرزت عن مخاطر لم تكن واقعة من قبل، وذلك عبر تزايد تدفق المعلومات والبيانات عبر شبكة الإنترنت، وأيضاً سهولة ربط الاتصالات ما بين الأشخاص في دول مختلفة، وبالتالي سهولة تشكيل روابط وعلاقات متنوعة سواء كانت مشروعة أو غير مشروعة، وهنا يظهر حق الدولة وأجهزتها في بسط الرقابة على هذا المجال الحساس، خاصة عبر تزايد الأنشطة الإجرامية العابرة للحدود عبر استغلال هذه الشبكة العنكبوتية، ولعل هذا الأمر ما ساعد في نسبية الحق في سرية الحياة الخاصة أو الخصوصية المعلوماتية، والتي من بينها لتنفيذ مهمة تدخل ضمان الصالح العام أو من أجل ضمان ممارسة مهام السلطة العامة التي يتولاها المسؤول عن المعالجة، أو لتحقيق مصلحة مشروعة من قبل المسؤول عن

(1) إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث، 2004، ص1004.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

المعالجة وعليه فإن حماية الحق في الخصوصية يقع بين حق الفرد في الحياة الخاصة، وبين إلزامية الاطلاع على شؤون الأفراد وما تفرضه من ضرورة المصلحة العامة؛ لأن مجال الاتصالات الإلكترونية، صار ملاذاً ملائماً لهذه الممارسات والأفعال الإجرامية المتنوعة، وبالتالي تبسط الدولة رقابتها عليها[1].

### 5. ظهور مخاطر جديدة

ان ما شهده التطور التكنولوجي حديثاً، الذي أفرز معه مخاطر جديدة عبر تكاثر نسبة وحجم المعلومات والبيانات الشخصية المفرزة والمخزنة والمرسلة عبر الإنترنت، صار معه أيضاً مجال حق الخصوصية واسعاً وأشمل مما كان عليه، ولعل هذا الأمر هو الذي ساعد على ظهور مخاطر جديدة تحاول المساس بهذه الخصوصية المعلوماتية التي أصبحت متاحة للجميع، سواء عن طريق مواقع التواصل الاجتماعي أو عن طريق البريد الالكتروني، فمثلاً قد يلجأ المستهلك الإلكتروني للتعاقد عبر أحد المواقع التجارية الالكترونية أو عن طريق البريد الالكتروني، أو يقوم شخص معين بإنشاء حساب في أحد مواقع التواصل الاجتماعي، فيأتي أحد من الغير، سواء تربطه علاقة به أو لا، يحاول الولوج إلى تفاصيل المراسلات والاتصالات أو حتى المكالمات، أو البحث عن تفاصيل حياته أو بياناته الشخصية, لأن تلك الأجهزة تحتوي على بيانات كثيرة، تتعلق بحريته الفردية كالحالة الاجتماعية، والانتماءات السياسية، والحالة الوظيفية والقيود الجنائية، في حالة وجود أحكام أو سوابق عدلية، ويحاول بكل الطرق والوسائل المتاحة عبر هذا الفضاء الرقمي للكشف عنها والوصول إليها، والتي سهلت من ظهورها الاتصالات الإلكترونية[2]، وهنا ظهرت المخاطر الالكترونية، كالقرصنة والفيروسات والبريد الإلكتروني غير المرغوب فيه، والتجسس على البيانات الشخصية، والحصول على كلمات السر بطريقة غير مشروعة واستخدام بريد الكتروني لشخص معين، كذلك سرقة المعلومات الخاصة كبطاقات الائتمان من خلال التسلل الالكتروني او اي وسيلة من وسائل وتطبيقات التكنولوجيا الحديثة كذلك مخاطر التطور الهائل للذكاء الاصطناعي، مع مراعات كثرة الاستخدامات لهذه التطبيقات من قبل الافراد، وقد تكشف التطورات الخاصة بالرقمنة مخاطر جديدة لم تظهر بعد.

(1) بعجي احمد، تطور مفهوم حماية الحق في الخصوصية، بحث منشور، مجلة القانون والمجتمع، العدد1، المجلد الثامن، الجزائر، 2020، ص459.

(2) شيماء عبد الغني عطاء الله، تراجع الحق في الخصوصية في مواجهة الاتصالات الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد 10، السنة الثالثة، يونيو 2015، ص 503.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

## المطلب الثاني

## القيود الجنائية على حماية الحق في الخصوصية المعلوماتية

ان الحق في الخصوصية المعلوماتية يتمتع بحماية جنائية كبيرة ضمن التشريعات العراقية وتحديداً ضمن قانون العقوبات العراقي رقم 111 لسنة 1969، حيث جرم القانون العديد من الأفعال التي تنتهك او تمس الحق في الخصوصية، اذ ان الهدف من القانون هو إمكانية تحقيق توازن بين حق الدولة في توفير حماية للمجتمع وبين حماية حق الافراد في الحريات الفردية، الا ان ذلك التعارض حقق قيداً على حقوق وحريات الافراد كما في حالة ارتكاب الجرائم والكشف عن المجرمين، وكذلك إمكانية تحقيق رقابة على الحق في الخصوصية من خلال ضبط المراسلات او مراقبة الاتصالات الهاتفية للكشف عن الجريمة.

فحق الفرد في حماية حقه في الخصوصية المعلوماتية يقتضي توفير ضمانة من الاعتداء عليه او التدخل او الانتهاك، وهو حق مكفول قانوناً للجميع سواء كانوا افراداً عاديين او من افراد السلطات العامة، لكن هذا الحق ليس مطلقاً بل مقيداً بقيود قانونية[1].

وتجري التشريعات عموماً الى تقسيم المحادثات الى عامة وخاصة وتمنع تلك التشريعات مراقبة الاحاديث الخاصة الا بشروط وضمانات قانونية، ومع التطور العلمي الحديث في مجال الاثبات الجنائي، ظهر الدليل الالكتروني من افضل الأدلة في الجرائم المعلوماتية، حيث انه يتمتع بحجية علمية في الاثبات وذلك كونه محكم بقواعد قطعية، ويقصد بالدليل الالكتروني في الاثبات "هو البيانات التي يمكن اعدادها وارسالها وتخزينها بحيث تمكن الحاسب الالي من تنفيذ مهامه وتساعده في كشف الجرائم مثل التسجيل الصوتي، والكاميرات والصور وغيرها" [2].

كذلك ان التسجيل الذي يتم قبل وقوع الجريمة تكون له صفة امنية وإدارية وليست قضائية بسبب عدم توفر صفة الخصومة في قيمة الدليل الالكتروني الذي يتم بواسطة التسجيل الصوتي، الا ان الفقه لم يتفق على رأي موحد في شرعية التسجيل الصوتي كدليل رقمي لإثبات الجريمة، اما الفقه القانوني العراقي فقد اتجهوا الى رفض الاعتماد على التسجيل الصوتي كدليل للأثبات الجنائي، وذلك لإنه يتعارض مع الضمانات القانونية والدستورية للأفراد ويتعارض مع الحق في الخصوصية الذي كفله الدستور[3]، وهنالك اتجاه اخر يذهب مع تأييد الاعتماد على التسجيل الصوتي كونه احد الوسائل التي

(1) لؤي عبد الله نوح، مدى مشروعية المراقبة القانونية الالكترونية في الاثبات الجنائي، مركز الدراسات العربية، القاهرة، 2018، ص97.

(2) خالد حسن احمد لطفي، الدليل الرقمي ودوره في اثبات الجريمة المعلوماتية، دار الفكر الجامعي، 2019، ص55.

(1) اثير ذياب عباس، مشروعية الوسائل الرقمية في كشف الجرائم وأثرها في الحق في الخصوصية، رسالة ماجستير، كلية القانون، جامعة ديالى، 2024، ص64.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

تؤدي للحصول على الأدلة لكشف الجرائم، وبين الاتجاهين السابقين ورد اتجاه ثالث وهو ما نرجحه ويذهب معه الفقه القانوني العراقي في اغلب تعاملاته يرى ان الحماية القانونية والدستورية للاتصالات غير مطلقة فيمكن الكشف عنها وتسجيلها على ان يكون في أواصر قانونية وقضائية.

اما قانون أصول المحاكمات الجزائية العراقي رقم 23لسنة 1971 فقد عطى سلطة تقديرية للقاضي اثناء التحقيق، وهذا يدل على ان الحق في الخصوصية ليس مطلقاً دائماً ففي حالة الجرائم والتحقيق يجوز ان يلزم الافراد على تقديمها وهذا لا ينتهك الحق في الخصوصية، فمن الطبيعي ان يتمكن قاضي التحقيق من الاطلاع على المراسلات والوثائق او ان يأمر بمراقبة مكالمات هاتفية لأشخاص معنيين متى ما كان ذلك يسهل من عملية الكشف عن ملابسات الجريمة.

ان المشرع العراقي عند وضع النص السابق لم يذكر بشكل صريح ماهية الوسائل الالكترونية التي تساعد في الاثبات الجنائي، مما يجعل من الممكن اعتماد التسجيل الصوتي في الاثبات، الا ان هنالك تردد قضائي في ذلك وقد ذهب جانب من الفقه المصري الى تأييد قبول التسجيل الصوتي في الاثبات الجنائي[1].

اما في التشريعات الفرنسية نجد ان محكمة النقض الفرنسية اقامت مشروعية المراقبة على المكالمات والمحادثات الهاتفية قبل صدور القانون رقم (91-646) لسنة 1991 مستندة في ذلك احكام قانون الإجراءات الجنائية الفرنسي، حيث تشدد المحكمة على بطلان التنصت على المكالمات الهاتفية اذا تم بوسائل الغش او الخداع وتؤكد على وجوب صحة الإجراءات وان تكون خالية من الوسائل او الممارسات الاحتيالية سواء أجريت من قبل قاضي التحقيق او مأمور الضبط القضائي، على ان تراعى بذلك عدم مخالفة نص المادة(8) من الاتفاقية الاوربية لحقوق الانسان لعام 1950 التي اكدت على حماية الحياة الخاصة[2]، ومن امثلة نماذج الغش والاحتيال المعلوماتي ذات الطابع الجنائي.

### 1. اختلاس النقود

يرى الخبراء ان بإمكان أي شخص يشغل مركزاً على قدر كبير من الأهمية في احدى المؤسسات او البنوك، ويمتلك الخبرة الفنية في مجال استعمال الحاسب الالي، ان يختلس ما يشاء من معلومات يرغب فيها، بغية تحقيق اختلاس المبالغ المالية والحسابات الضخمة منتهزاً ضعف المراقبة في اغلب الأحيان، ومن الأمثلة التطبيقية على ذلك ما يأتي.

(2) عمار عباس الحسيني، التصوير المرئي والتسجيل الصوتي وحجيتهما في الاثبات الجنائي، المركز العربي للنشر والتوزيع، القاهرة، 2017، ص182.

(3) ايلاف نصرة فارس، حماية الحق في الخصوصية الرقمية في ظل القانون الدولي والتشريعات الوطنية، رسالة ماجستير، جامعة ديالى، كلية القانون، 2026، ص145.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

- قيام شرطة مرسيليا الفرنسية بالقبض على مستخدم يعمل لدى فرع مصرف تابع لبنك Indo-Suez تمكن من اجراء تحويلات لنقود وهمية مستخدماً في ذلك الحاسب الخاص بالبنك، اما المبالغ فأنها لم ترد في الخزينة الخاصة بالبنك الا انها سجلت في ذاكرة الحاسب الالي قبل ان تنتقل بواسطة محررات خاصة مصطنعة الى حساب فتح باسمه في سويسرا، وقد وجهت له الأجهزة الأمنية تهمة اختلاس سبعة مليون فرنك فرنسي[1].

### 2. الدخول غير المشروع:

تشكل جريمة الدخول غير المشروع الى التطبيقات الخاصة تعدياً على الحق في الخصوصية، ويقصد به الدخول او الوصول الى غاية او هدف معين بطريقة غير قانونية من خلال استغلال الثغرات الموجودة في النظام او التشفير، في حين عرفه اخرون، الولوج غير المسموح به او غير المصرح به الى الأجهزة الالية الخاصة بالغير وشبكاتهم المعلوماتية من خلال استخدام تقنيات حديثة اعدت لهذا الغرض.

### 3. جريمة اصطناع حساب خاص:

نصت بعض القوانين التي تكافح الجريمة المعلوماتية على هذه الجريمة ومن ذلك قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لعام ٢٠١٨ ومستند هذه الجريمة هو نص المادة (24) والتي تناولت النص على هذه الجريمة من خلال العقاب بالحبس لكل من يقوم باصطناع البريد الإلكتروني أو الحسابات الخاصة أو المواقع الشخصية ومن ثم ربطها بأشخاص طبيعيين أو اعتباريين، ويتم تشديد العقوبة في حال تم استخدام هذا البريد المصطنع او الحساب الخاص في ما يسبب إساءة للشخص المنسوب له وكذلك يشدد العقوبة إذا وقعت الجريمة على الأشخاص الاعتباريين.

للجريمة ركنين مادي ومعنوي : فأما الركن المادي فيقوم على سلوك قوامه اصطناع بريد إلكتروني أو موقع أو حساب خاص، ووفقاً لقانون مكافحة جرائم تقنية المعلومات المصري عُرف الموقع بأنه: نطاق أو مكان افتراضي له عنوان محدد على شبكة معلوماتية وكذلك القانون السوري فلقد عرفه بأنه منظومة ذات اسم وعنوان يتم تعريفها على الشبكة المعلوماتية ويحتوي على بيانات ومعلومات وخدمات يتم الوصول إليها من خلال الشبكة العالمية وبخاصة الانترنت فالمواقع الإلكترونية هي عبارة عن صفحات ترتبط ارتباطاً كاملاً بالإنترنت وتخصص عادة من قبل شخص ما أو شركة ما لعرض مواضيع مرتبطة فيما بينها ووثيقة

(1) الجريمة السيبرانية، محمد عبد الله أبو بكر سلامه، دار الكتب والدراسات العربية، القاهرة، 2023، ص111.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

الصلة ويمكن لأصحابها بث المواد التي يريدونها، والاصطناع الذي يقوم به الركن المادي لهذه الجريمة يعني إظهار شيء من العدم أو إيجاد شيء لم يكن موجودا ، وهو تغيير الحقيقة أيا كان موضوعه وأيا كانت وسيلته[1]، واصطناع البريد بصورة عامة يتم بإحدى طريقتين، **الأولى** : وهي طريقة مجانية بمقتضاها يتم إنشاء البريد عن طريق الدخول إلى موقع يقدم هذه الخدمة مجاناً ، ثم تقديم المعلومات التي تريدها الشركة المزودة للخدمة والتي بتقديمها يتم الإنشاء التلقائي للموقع، اما **الطريقة الثانية**[2]**:** وفقا لهذه الطريقة يتم إنشاء البريد من خلال دفع رسوم مالية زهيدة ووفق ترتيب إجرائي محدد، تبدأ بحجز مجال للبريد يتم شراؤه ثم تصميم صفحات من قبل مهندس متخصص، ومن ثم في الموقع مقابل مبلغ معين وعندما تعمد إحدى الشركات إلى إنشاء موقع ما لأحد عملائها تقوم باستخدام جهاز خدمة أمن server secure وبمقتضاها تتفق الحاسبات على استخدام رموز مشفرة تستخدم تأمين البيانات . وأما الركن المعنوي فتعتبر جريمة اصطناع الحساب الشخصي من الجرائم المقصودة والتي يقوم ركنها المعنوي على القصد الجنائي بعنصريه العلم والإرادة فيلزم أن يكون الجاني عالما بأن الحساب الذي يصطنعه هو حساب وهمي لأحد الأشخاص الطبيعيين أو الاعتباريين، وأنه سينسب الحساب المصطنع زورا إليه وأن تتجه إرادته إلى ذلك.

مما تقدم نجد ان الدليل الإلكتروني يحتاج الى رأي الخبير القضائي او الخبير المختص ومن ثم رأي قاضي الموضوع صاحب الحكم في الدعوى، اما رأي الخبير غير ملزم وان اقصى ما يمكن تحقيقه هو محاولة اقناع القاضي، إضافة لما تقدم نجد ان القيود التي ترد على الحق في الخصوصية المعلوماتية هي امراً محظوراً، لإنه اجراء يتعارض مع حقوق الافراد والحريات العامة، فمن الضروري ان يكون هنالك توازن وتوفيق في حق الافراد بعدم انتهاك خصوصيتهم وحق الدولة في المحافظة على النظام العام من خلال المراقبة.

(1) بهاء المري، شرح جرائم تقنية المعلومات، منشأة المعارف، الإسكندرية، مصر، 2019، ص215.
(2) فرج الله المقداد، الحماية الجزائية للبريد الالكتروني، رسالة ماجستير، جامعة دمشق، كلية الحقوق، 2022، ص77.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

## المطلب الثالث

## امكانية تطوير الحماية الدولية للحق في الخصوصية المعلوماتية

### اولاً: مواجهة صعوبات التعاون الدولي

فيما يتعلق بصعوبة عدم وجود نمط موحد للنشاط الاجرامي: فإن الأمر يقتضي توحيد هذه النظم القانونية، ولاستحالة هذا الأمر فإنه لا مناص من البحث عن وسيلة أخرى تساعد على إيجاد تعاون دولي يتفق مع طبيعة هذا النوع المستحدث من الجرائم وبالتالي يخفف من حدة الفوارق بين الأنظمة العقابية الدولية، وتتمثل هذه الوسيلة في تحديث التشريعات المحلية المعنية بالجرائم المعلوماتية و إبرام اتفاقيات خاصة سواء كانت ثنائية ام متعددة الاطراف او حتى الشارعة منها يراعي فيها هذا النوع من الجرائم ، وان تتم مراجعة لهذه الإتفاقيات بصفة دورية[1].

اما فيما يتعلق بتنوع واختلاف النظم القانونية الإجرائية نجد أن المواثيق الدولية الصادرة عن الأمم المتحدة غالبا ما تشجع الأطراف فيها على السماح باستخدام بعض تقنيات التحقيق الخاصة، الشيء الذي يخفف من غلو واختلاف النظم القانونية والإجرائية ويفتح المجال أمام تعاون دولي فعال , فنجد نص المادة (20) من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية تشير في هذا الصدد إلى التسليم المراقب والمراقبة الإلكترونية وغيرها من أشكال المراقبة والعمليات المستترة، والتي تعتبر من أهم التقنيات المستخدمة في التصدي للجماعات الإجرامية المنظمة، بسبب الأخطار والصعوبات الكامنة وراء محاولة الوصول إلى عملياتها وتجميع المعلومات وأدلة الإثبات لاستخدامها فيما بعد في الملاحقات القضائية المحلية منها أو الدولية في دول أطراف في سياق نظم المساعدة القانونية المتبادلة[2].

ومن خلال استقراء نصوص الاتفاقيات الدولية في هذا المجال نجد ان الاتفاقية الأوربية للإجرام المعلوماتي اكدت من حيث النص للمواد (31,32,33,34) على سرية حفظ البيانات المعلوماتية المخزنة وأجازت لكل طرف أن يطلب من الطرف الآخر الحفظ السريع للمعلومات المخزنة عن طريق إحدى الوسائل الإلكترونية الموجودة داخل النطاق المكاني لذلك الطرف الآخر والتي ينوي الطرف طالب المساعدة أن يقدم طلبا للمساعدة بشأنها بغرض القيام بالتفتيش أو الدخول بأي طريقة مماثلة، وضبط أو الحصول أو الكشف عن البيانات المشار إليها.

(1) محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، مصدر سابق، ص117.
(2) تحليل نص المادة (20) ، اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

نلحظ مما تقدم ان الاتفاقية الاوربية للاجرام المعلوماتي ومنظمة الامم المتحدة في مكافحة الجريمة المعلوماتية، اوجدت بعض الحلول من اجل التغلب على اشكالية اختلاف النظم الاجرائية امام التعاون الدولي لمواجهة جرائم المعلوماتية.

اما القيد الثالث والمتعلق بظاهرة عدم وجود قنوات اتصال بين جهات إنفاذ القانون فنلحظ أنه غالبا ما تشجع المواثيق الدولية الدول إلى التعاون فيما بينها وتدعوها إلى إنشاء قنوات اتصال بين سلطاتها المختصة ووكالاتها ودوائرها المتخصصة بغية التيسير في الحصول على هذه المعلومات وتبادلها، ومن الأمثلة على هذه المواثيق الدولية اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية في المادة (27) منها والمادة (9) من اتفاقية 1988م والمادة (48) من اتفاقية الأمم المتحدة لمكافحة الفساد والبند الثاني من المادة (27) من الاتفاقية الأوربية بشأن الإجرام المعلوماتي، والمادة (35) من ذات الاتفاقية الأوربية والتي أوجبت على الدول الأطراف فيها ضرورة تحديد نقطة اتصال تعمل لمدة 24 ساعة يومياً طوال أيام الأسبوع لكي تؤمن المساعدة المباشرة للتحقيقات المتعلقة بجرائم البيانات والشبكات أو استقبال الأدلة ذات الشكل الإلكتروني، وهذه المساعدة تشمل تسهيل أو إذا سمحت الممارسات والقوانين الداخلية بذلك تطبيق الإجراءات التالية بصفة مباشرة( إسداء النصيحة الفنية- حفظ البيانات وفقاً للمواد 29-30 جمع الادلة واعطاء المعلومات ذات الطابع القضائي وتحديد اماكن المشتبه بهم).

أما بالنسبة للقيد الرابع والمتعلق بمشكلة الاختصاص في الجرائم التي تتم عبر شبكات الانترنت فهالك ضرورة ملحة إلى إبرام اتفاقيات دولية ثنائية كانت أو جماعية يتم فيها توحيد وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي خاصة بالنسبة للجرائم المتعلقة بالإنترنت، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرائية بما يتناسب والتطور الكبير التي تشهده تكنولوجيا المعلومات والاتصالات.

اضافة لما تقدم بالإمكان نتائج أفضل وبالتالي تحقيق التغلب على الصعوبات الفنية التي تواجه التعاون الدولي، من خلال ابداء جهود أكثر فيما يتعلق بالدورات والبرامج التطويرية لتحقيق قدر اعلى من الحماية ازاء الجرائم المعلوماتية، يتركز نشاط هذه الدورات على افراد القانون وبجميع الفئات سواء كانت افراد الادلة الجنائية ام المساعدين القضائيين ام غيرهم من الافراد ذوو الاختصاص في هذا مجال الجرائم المعلوماتية.

### ثانياً: مواجهة المعوقات الداخلية

ان **الحق في الخصوصية المعلوماتية حق دستوري**: اي انه يعنى بحماية دستورية هامة، فنجد أن هناك عدة أحكام تنص على مختلف صور الحق في الخصوصية، فمثلاً تنص المادة (17) من الدستور العراقي


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

النافذ "لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الاخرين والآداب العامة"[1]، وكذلك اكد الدستور على سرية المراسلات وعدم جواز الاطلاع عليها او مراقبتها او التنصت عليها الا بموافقة قضائية وفقاً للقانون, كذلك تأكيد قانون العقوبات العراقي على واجب الحماية لسرية المراسلات والاتصالات وتجريم افشاء الاسرار، جرائم القذف والتشهير, الاعتداء على حرمة المساكن، وبالرغم من عدم ادراج نصوص صريحة على الخصوصية المعلوماتية الا انها لا تخرج عن مفهوم الخصوصية بصورة عامة، لكن حديثاً، أدرك المشرع الدستوري أهمية تأثير وسائل الرقمنة والتكنولوجيا على حياة الأفراد وخصوصياتهم، وهو ما بادر الى التركيز من خلال عقد الندوات والورش والتشجيع في كتابة البحوث التي توفر نوعا من الحماية للخصوصية المعلوماتية من خلال تثقيف الجمهور والتنبؤ بخطورة الرقمنة وتحديد المسؤولية الناتجة عنها.

### ثالثاً: الامن السيبراني ضمانة هامة لتفعيل الحماية

يعد الامن السيبراني أحد اهم وسائل ضمانات حماية الحق في الخصوصية المعلوماتية، فهو ذات طبيعة استراتيجية وتقنية تعمل على تأمين البيانات وامكانية الدخول لها ومعالجتها او نقلها الكترونياً وتهدف سياسة الامن السيبراني الى مجموعة من الامور اهمها:

- تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم لحماية نظم الكمبيوتر والشبكات، كذلك حماية المعلومات والبيانات الشخصية وغير الشخصية في مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة استرجاعها.
- وضع آليات وتدابير لمكافحة تسريب المعلومات أو الدخول غير الآمن لها من خلال البرامج الإلكترونية التي تدعم تلك الحماية للبيانات الشخصية.
- وضع استراتيجية لخصوصية البيانات الشخصية، وعدم تعرضها لخطر الإفشاء، بالإضافة إلى سلامة المحتوى، والتي يقصد بها أن البيانات محل الحماية بيانات صحيحة لم يتم تعديلها أو العبث بها أو لم يتم إتلاف محتوى المعلومات عن طريق التدخل غير المشروع أو غير القانوني لمعالجة البيانات الشخصية[2].

---

(1) كما لم يقتصر الأمر على الإهتمام الداخلي للدول بمسألة الخصوصية المعلوماتية، بل أيضاً على الصعيد الدولي، فعلى سبيل المثال جاء في تقرير الجمعية العامة للأمم المتحدة سنة 2014، في قرار لها رقم (167/68) بتاريخ 19 نوفمبر 2014 في الدورة التاسعة والستين بشأن الحق في الخصوصية في العصر الرقمي على أن: "حق الإنسان في الخصوصية الذي لا يسمح بتعريض أي شخص لتدخل تعسفي، أو غير قانوني في خصوصياته، أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخل، وكذلك الحرص على أهمية الاحترام التام لحرية الحصول على المعلومات وتلقيها ونقلها للغير.

(2) رفعت شميس العراقي، الأمن المعلوماتي بين القرصنة والإرهاب الإلكتروني، شبكة موسوعة دهشة 2007، ص 158.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

اما المنظور القانوني، فإن الأمن السيبراني هو محل دراسات وتدابير حماية سرية وسلامة المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها، الا أن الأمن السيبراني لا يتحقق إلا من خلال توفير الحماية المتكاملة لقطاعي المعلومات والكمبيوتر، ويتخذ الأمن السيبراني عدة أنماط متعددة، منها: أولا : الحماية المادية، وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالإقفال والحواجز والغرف المحصنة. ثانيا: الحماية الشخصية، وهي تلك التي تتعلق بالموظفين العاملين على النظام التقني المعني، من حيث التعريف بوسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل مخاطر الاعتداء على المعلومات. ثالثا : الحماية الإدارية والمقصود منها سيطرة جهة الإدارة على إدارة نظم المعلومات وقواعدها، مثل: التحكم بالبرمجيات الخارجية والأجنبية عن المنشأة ومسائل الإشراف والرقابة والمتابعة وأخيرا الحماية المعرفية، كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة والخاصة [1].

مما تقدم نلحظ ان مخاطر الفضاء السيبراني أصبحت تشكل خطرا كبيرا في ظل انعدام الرقابة المهنية على الخصوصية المعلوماتية، كعمليات الابتزاز من قبل المخترقين وسارقي الهويات من خلال طلب المال أو تنازلات تؤدي إلى إغراق الضحية، والمحاربة كل أشكال الجريمة الإلكترونية من الابتزاز والفدية والتجسس والهجوم.. وغيرها؛ لذا يجب تطبيق سياسة الأمن السيبراني وأنظمة الحماية البرمجية والمادية لتحديد الإجراءات الدفاعية والوقائية لحمايتها من أي اختراق أو تخريب ومقاومتها حال وقوعها بهدف التقليل والحد من آثارها.

## رابعاً: تعزيز دور الامم المتحدة في حماية الخصوصية الرقمية.

بذلت الامم المتحدة العديد من الجهود من أجل حماية الحق في الخصوصية الرقمية من أي اعتداء تتعرض له، وقد اصدرت العديد من القرارات التي تتعلق بحماية الحق في الخصوصية الرقمية وهي تتمثل بما يلي:

### 1. القرار رقم (٦٨ / ١٦٧) المتعلق بحماية الحق في الحياة الخاصة في العصر الرقمي:

أصدرت الجمعية العامة للأمم المتحدة قراراً يتعلق بالخصوصية الرقمية في الثامن عشر من كانون الأول عام (٢٠١٣)، اذ افصح القرار عن القلق الكبير بشأن قدرة المؤسسات الحكومية المتزايدة على

(1) منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة ، 2013، ص306.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

الوصول إلى خصوصية الأفراد[1]، وقد أتى القرار في اتجاهين, الأول منهما تأكيد حق الأفراد في الخصوصية في ظل التقدم التكنولوجي، اذ أشار القرار في الفقرة الثانية من ديباجته إلى ما نصت عليه المادة الثانية عشرة من الإعلان العالمي لحقوق الإنسان والمادة (١٧) من العهد الدولي للحقوق المدنية والسياسية[2] .

اما بشأن الحق في الخصوصية الرقمية، فأن ابرز ما جاء به القرار في حماية هذا الحق، هو تأكيده من جديد على حق الإنسان في الخصوصية، اذ لا يسمح بتعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أو في شؤون أسرته أو بيته أو مراسلاته، وحقه في التمتع بحماية القانون من مثل هذا التدخل، وإن ممارسة الحق في الخصوصية أمر مهم لإعمال الحق في حرية التعبير والحق في اعتناق الآراء دون مضايقة، فضلاً عما جاء بتقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير المقدم إلى مجلس حقوق الإنسان في دورته الثالثة والعشرين بشأن تداعيات مراقبة الدول للاتصالات على ممارسة حق الإنسان في الخصوصية وحقه في حرية الرأي والتعبير، وإذ تشدد على أن مراقبة الاتصالات و أو اعتراضها على نحو غير قانوني أو تعسفي وجمع البيانات الشخصية على نحو غير قانوني أو تعسفي أمور تنتهك الحق في الخصوصية والحق في حرية التعبير وقد تتعارض مع مبادئ المجتمع الديمقراطي بالإضافة الى التداعيات السلبية على ممارسة حقوق الإنسان والتمتع بها من جراء مراقبة الاتصالات و أو اعتراضها، بما في ذلك مراقبة الاتصالات خارج إقليم الدولة أو اعتراضها وكذلك جمع البيانات الشخصية[3].

### 2. القرار رقم (166/٦٩) المتعلق بحماية الحق في الحياة الخاصة في العصر الرقمي

وفقاً لتقرير المفوضية السامية للأمم المتحدة لحقوق الإنسان الصادر عام ٢٠٢٢، أفادت الأمم المتحدة بتاريخ ١٦ أيلول / سبتمبر ٢٠٢٢ بأن الحق في الخصوصية يشهد انتهاكاً متزايداً وتعرضاً لضغوط غير مسبوقة نتيجة التطور المتسارع في التقنيات الرقمية المرتبطة بالشبكات، والتي تستخدم بوصفها أدوات فعالة للمراقبة، وقد تناول التقرير ثلاث قضايا جوهرية تمس الخصوصية الرقمية وهي إساءة

(1) قرار الامم المتحدة رقم (167/68) بتاريخ ١٨ تشرين الأول لسنة ٢٠١٣ ، الدورة ٦٨ البند ٦٩ (ب) ./A/RES/73/16

(2) نصت المادة (١٢) من الاعلان العالمي لحقوق الانسان على أن لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته، فيما نصت المادة (١٧) من العهد الدولي للحقوق المدنية والسياسية ١- لا يحوز تعريض أي شخص على نحو تعسفي أو غير قانوني لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته ٢- من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس.

(1) قرار الامم المتحدة رقم (167/68) بتاريخ ١٨ تشرين الأول لسنة ٢٠١٣, الدورة ٦٨ البند ٦٩ (ب) ./A/RES/73/16


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

استخدام السلطات الحكومية لبرمجيات الاختراق والتجسس الإلكتروني، الأهمية البالغة لتوفير نظم تشفير قوية كوسيلة لحماية حقوق الإنسان في الفضاء الرقمي الآثار المترتبة على التوسع في استخدام تقنيات المراقبة في الأماكن العامة، وأكد التقرير ضرورة اتخاذ إجراءات عاجلة للتصدي لانتشار واستخدام برمجيات التجسس، داعياً إلى اعتماد ضمانات قانونية ملزمة تكفل احترام حقوق الإنسان وحمايتها، كما شدد على أن لجوء السلطات إلى وسائل الاختراق الحاسوبي للأجهزة الشخصية يجب أن يكون مشروطاً بكونه تدبيراً أخيراً، لا يستخدم إلا في حالات استثنائية تستدعي منع أفعال تشكل تهديداً جسيماً للأمن القومي[1].

و في سياق التطورات التقنية المتسارعة التي يشهدها العالم صدر تكليف عن المفوض السامي لحقوق الإنسان، بإعداد تقرير يتناول مسألة حماية الحق في الخصوصية وتعزيزه، و تقرر أن يُعرض هذا التقرير على كل من مجلس حقوق الإنسان والجمعية العامة للأمم المتحدة وفي عام ٢٠١٤، أنجز هذا التقرير تحت عنوان الحق في الخصوصية في العصر الرقمي"، وقد اعتبر بمثابة خطوة جوهرية في سبيل توضيح وتفسير موقف القانون الدولي من الحق في الخصوصية، لا سيما في ظل التحديات التي تفرضها الوسائل الرقمية الحديثة[2].

ولقد كان هدفه وضع واقع قانوني يمكن أن ينشط خلال إطار واضح ومباشر يساهم بفاعلية في حماية الحق في الخصوصية في ظل التطور التكنولوجي والقدرة غير المحدودة للدول على مراقبة الأفراد. وقد قدم التقرير عنصرين أساسيين: الأول هو استقراء الممارسات باعتبارها نقطة انطلاق لتشكيل الغرف الدولي كمصدر رئيسي للقانون الدولي العام، والثاني هو ان يكون هناك توازن بين هذه الممارسات والموقف التقليدي لقواعد القانون الدولي المتعلقة بالخصوصية، وانتهى التقرير للوصول الى أن المجتمعات الدولية بصورة عامة تشهد تزايداً في الاستخدام للتكنولوجيا في مختلف المجالات وبصورة يومية، بالإضافة إلى وجود خطر الإرهاب الدولي الذي يستخدم هذه الوسائل والحقوق لإخفاء أنشطته وما يسمى الارهاب السيبراني)، وقد أكد التقرير على أنه يمكن للدول استخدام برامج المراقبة الالكترونية ولكن يجب ان تلتزم بالشروط والتعليمات الرئيسية، مثل أن يكون برنامج المراقبة الإلكترونية مستنداً إلى قانون غير تعسفي صادر عن السلطة المختصة، وأن تكون المراقبة جائزة في بعض الحالات بشرط أن تتم بعيداً عن التمييز[3].

(2) مريم نباش، التجسس وانتهاك حق الخصوصية في العالم الرقمي (دراسة وصفية تحليلية لبرنامج بيغاسوس) ، بحث منشور، مجلة الدراسات الاعلامية والاتصالية، جامعة الجزائر ، كلية القانون، مجلد (٢) العدد (٣) ، ٢٠٢٢، ص 75.
(3) قرار الامم المتحدة رقم (٦٩ / ١٦٦) بتاريخ ١٨ كانون الأول2014، الدورة ٦٩، البند (٦٨ (ب) /A/RES/73/16.
(1) فتحية حزام، الحق في الحياة الخاصة في البيئة الرقمية، بحث منشور، مجلة الدراسات القانونية المقارنة، جامعة محمد بوقرة، كلية القانون، الجزائر، مجلد (٨) العدد (١) ، ٢٠٢٢، ص ١٢٨.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

### 3. القرار رقم (199/٧1) المتعلق بحماية الحق في الحياة الخاصة في العصر الرقمي

صدر عن الجمعية العامة القرار 199/71 بتاريخ2016/12/19، وقد أكد على ضرورة تعزيز واحترام حقوق الانسان وممارسة الفرد حقوقه على الانترنيت، والزامية احترام الدول بموجب القانون الدولي الحقوق الانسان وعلى وجه الخصوص فيما يخص جمع وحماية البيانات الحساسة لاعتبارات تتعلق بخصوصية الافراد وحماية النظام العام[1].

### 4. قرار رقم (179/73) المتعلق بحماية الخصوصية في العالم الرقمي

صدر هذا القرار في دورة انعقاد الجمعية العامة في بتاريخ 2018/12/17 , أكدت الجمعية العامة لأمم المتحدة في هذا القرار على الخطر الذي يمس الأفراد في العالم الرقمي، وبصورة خاصة النساء والاطفال، ويتطلب هذا الأمر اهمية احترام هذا الحق، وايضاً شددت على ضرورة احترام سرية الاتصالات والمراسلات وذلك باللجوء الى حلول تقنية مناسبة.

### 5. رقم الامم المتحدة رقم (176/75) المتعلق بحماية الخصوصية في العصر الرقمي

اعتمد هذا القرار في دورة انعقاد الجمعية العامة في بتاريخ 2020/12/16، بعد قرارتها السابقة عادت الجمعية العامة للأمم المتحدة الى تأكيد ما طلبته من الدول، وهو حماية الخصوصية الرقمية والاتصالات ويجب ان تتأخذ الدول التدابير الإلزامية لوضع حد لانتهاكات هذا الحق، كما وجهت الشركات الناشطة في مجال التكنولوجيا ومعالجة المعطيات الشخصية ان تؤدي التزاماتها فيما يخص احترام حقوق الانسان وتشجيع الشركات على وضع حلول تقنية تسمح بضمان المحافظة عل الخصوصية الرقمية للأفراد [2].

## الخاتمة

ان الحق في الخصوصية المعلوماتية في ظل الرقمنة يعد ذات اولوية في المجتمع الدولي , وبناءً على ذلك حظي بحماية خاصة ضمن الاتفاقيات والمؤتمرات الدولية، اذ اهتمت الامم المتحدة بالحق في الخصوصية والتأكيد على ضرورة توفير الحماية الدولية للحق، اما النطاق الاقليمي ايضاً اكد على ضرورة ايجاد نوع من الحماية ضمن الاتفاقيات الخاصة، كذلك اكدت التشريعات الوطنية على توفير الحماية للحق في الخصوصية المعلوماتية نظراً لما له اهمية على الحق في الحياة، وذلك سوف نوضحه

(2) ايلاف نصرة فارس، حماية الحق في الخصوصية الرقمية في اطار احكام القانون الدولي والتشريعات الوطنية، رسالة ماجستير، جامعة ديالى، كلية القانون والعلوم السياسية، 2026، ص83.

(1) ايلاف نصرة فارس، مصدر سابق ، ص83.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

من خلال استعراض اهم النتائج التي توصلنا في البحث، وادراج مجموعة من المقترحات التي نرى انها ضرورية لاستدامة الحماية للحق في الخصوصية المعلوماتية.

## اولاً: النتائج

1. ان الحق في الخصوصية المعلوماتية في ظل الرقمنة أصبح من اهم حقوق الانسان الحديثة والتي يجب توفير الحماية لها من قبل المجتمع الدولي.
2. ان مسألة الاقرار الصريح للحق في الخصوصية المعلوماتية لم يرد ضمن نصوص قانونية واضحة ومتكاملة، بل ورد ضمن الحق في الخصوصية بصفة عامة وذلك على الصعيدين الداخلي والدولي.
3. وجود قصور كبير في بعض التشريعات وخاصة العربية منها في مجال جريمة انتهاك الحق في الخصوصية المعلوماتية وعدم كفاية قواعد الحماية تجاه بعض الانتهاكات، ومنها القرصنة الالكترونية، والاختراق والتجسس الالكتروني.
4. وجود تقاطع وتعارض بين مصطلح الحق في الخصوصية المعلوماتية وبعض الحقوق مثل الحق في حرية الراي والتعبير والحق في الوصول للمعلومة وحق الدولة في الرقابة.
5. على الصعيد الداخلي وجدنا ان التشريعات العراقية لا تزال متاخرة في مجال توفير الحماية مقارنة بالعديد من الدول العربية والأجنبية، اذ لا توجد اجراءات فعلية ازاء الخصوصية المعلوماتية والذكاء الاصطناعي باعتبارهما من الموضوعات المستجدة، فلا توجد توجيهات او تعليمات مباشرة لمواجهة خطر التطور التكنولوجي والتقني.
6. على الصعيد الدولي وبالرغم من ضعف الاجراءات وعدم الزامية البعض منها الا ان هنالك جهود ضمن منظمة الامم المتحدة اذ صدر عنها مجموعة قرارات أشرنا لها ضمن البحث، عملت على معالجة بعض الانتهاكات التي حصلت ازاء الخصوصية المعلوماتية.

## ثانياً: المقترحات

1. ضرورة تكاتف الجهود الدولية والداخلية من اجل تقنين الحماية للحق في الخصوصية المعلوماتية والجرائم السيبرانية ضمن إطار القانون الدولي على شكل معاهدات دولية وإقليمية، او ابرام اتفاقيات ثنائية متخصصة في مواجهة جرائم المعلوماتية.
2. ضرورة خضوع مواقع التواصل الاجتماعي في معالجتها للبيانات ذات الطابع الشخصي للافراد لضوابط قانونية من خلال ادراج قانون موحد للجرائم المعلوماتية والامن السيبراني وحماية الحق في الخصوصية المعلوماتية.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

3. تكثيف الجهود الدولية الخاصة بحماية الحق في الخصوصية المعلوماتية بناءً على الانتهاكات المتزايدة والتحديات التي تتمثل في التطور السريع لوسائل التكنولوجيا الحديثة ويتم ذلك من خلال زيادة المؤتمرات الدولية المتخصصة وعقد دورات تدريبية للفئات العاملة في مجال الرقابة الرقمية، واقامة الورش والندوات التثقيفية، وتشريع اتفاقيات خاصة بمكافحة جرائم المعلوماتية، وضرورة إلزام الدول بتضمين هذا الحق ضمن تشريعاتها الداخلية من اجل منع التعدي على الخصوصية المعلوماتية.
4. ضرورة انشاء محاكم متخصصة بالجرائم السيبرانية، نظراً لصعوبة القضايا المتعلقة فيها وحاجتها لوجود خبراء متخصصين في مجال المعلوماتية، كما ينبغي تشديد عقوبات جرائم التعدي على الحق في الخصوصية المعلوماتية.
5. انشاء مراكز وطنية متخصصة تعمل على تحليل الجرائم المعلوماتية وما ينشر في مواقع التواصل الاجتماعي وشبكات الانترنت، والعمل على حجب المواقع التي تتعارض مع النظام والاداب العامة وتوفير بيئة عمل اعلامية وقائية تعمل من خلال تعزيز الثقافة العامة للجمهور.
6. ضرورة ادراج جرائم المعلوماتية والامن السيبراني ضمن المناهج العلمية في الكليات المتخصصة (الحقوق، الشرطة، العسكرية) من اجل توفير حماية أكثر وفهم أكبر للأمن المعلوماتي وبالتالي إمكانية تطوير البنية التحتية والانظمة المعلوماتية وتحقيق الامن القومي.

## قائمة المصادر

### اولاً:الكتب القانونية


1. آدم بديع آدم حسين، الحق في حرمة الحياة الخاصة ومدى الحماية التي يكفلها القانون الجنائي، دار النهضة العربية، القاهرة, 2011.
2. محمد عزت عبد العظيم، الجرائم المعلوماتية الماسة بالحياة الخاصة، الطبعة الأولى، دار النهضة العربية، القاهرة 2016.
3. يولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت, 2009.
4. نديم عبده، أمن الكمبيوتر: الفيروسات والقرصنة المعلوماتية وانعكاساتها على الأمن القومي، دار الفكر للأبحاث والدراسات، الطبعة الأولى، بيروت، 1991.
5. حسنين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، القاهرة , 2006.



Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

6. عادل السيد محمد علي، الحماية الدستورية للامن السيبراني، دار الكتب والدراسات العربية, 2024.
7. بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني: دراسة مقارنة، كلية الحقوق، جامعة الشرق الأوسط، 2017.
8. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط , 1994.
9. محمد لطفي عبد، الجرائم المعلوماتية: التحديات والحلول، كلية الملك فهد الامنية، الرياض, 2007.
10. بولين انطويوس ايوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت, 2009.
11. أسامة أبو الحسن مجاهد، حماية المصنفات على شبكة الإنترنت، دار النهضة العربية، القاهرة, 2010.
12. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر، دار الكتب القانونية، القاهرة, 2002.
13. محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، مركز الدراسات العربية، مصر, 2015.
14. عبد الله محمد صالح الشهري، المعوقات الإدارية في التعامل الأمني مع جرائم الحاسب الآلي: دراسة مسحية على الضباط العاملين بجهاز الأمن العام بمدينة الرياض، جامعة الملك سعود، الرياض، المملكة العربية السعودية, 2002.

**ثانياً: الاطاريح**

1. يسرى عبد الله عبد الباري عبد المطلب، الحماية المدنية الخصوصية المعلوماتية، اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2016.
2. عبد الرحمن محمد عبد المحسن الصفتي، دور الشرطة في التأمين التقني للعقود الالكترونية، اطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، 2017.

**ثالثاً: الرسائل**

1. خلاف بيرو، تطور حماية الحياة الخاصة للعامل، مذكرة لنيل شهادة الماجستير في الحقوق، تخصص تحولات الدولة، كلية الحقوق والعلوم السياسية، جامعة قصدي مرباح، ورقلة، 2010.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

2. محمد بن حيدة، الحق في الخصوصية في التشريع الجزائري (دراسة مقارنة)، مذكرة لنيل شهادة الماجستير، تخصص حقوق وحريات، قسم العلوم القانونية والإدارية، كلية الآداب والعلوم الإنسانية، الجامعة الإفريقية العقيد أحمد دراية , 2009.
3. بسمة بوكروم وايمان بوفليغة، الحق في الخصوصية في ظل الرقمية، رسالة ماجستير، جامعة محمد الصديق بن يحيى، كلية الحقوق والسياسة, 2019.
4. ايلاف نصرة فارس، حماية الحق في الخصوصية الرقمية في إطار احكام القانون الدولي والتشريعات الوطنية، رسالة ماجستير، جامعة ديالى، كلية القانون والعلوم السياسية, 2026.

**رابعاً: البحوث المنشورة**

1. نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الجزائي الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت المنعقد في كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة , 2000.
2. يونس غرب، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، منتدى العمل الإلكتروني بواسطة الهاتف الخلوي اتحاد المصارف العربية، عمان، الأردن 2002.
3. خدوجة الذهبي، حق الخصوصية في مواجهة الاعتداءات الإلكترونية: دراسة مقارنة، المجلد الأول، العدد الثامن، مجلة الاستاذ الباحث للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف بالمسيلة، الجزائر, 2017.
4. رؤى سعد القرني، تعزيزات لوصول في الخصوصية المعلوماتية: دراسة مقارنة، العدد السادس، مجلة كلية الدراسات الإسلامية والعربية للبنات بدمنهور، 2021.
5. عزت عبد المحسن إبراهيم، سلامة الحق في الخصوصية الرقمية وتحديات عصر التقنية، العدد الأول، مجلة العلوم الاقتصادية والقانونية، كلية الحقوق، جامعة عين شمس، يناير 2020.
6. ليتم فتيحة، ليتم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، العدد الثاني عشر، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة الجزائر، مارس 2015.
7. جميل زكريا محمود، الجريمة المعلوماتية واساليب التأمين، المؤتمر الدولي لأمن المعلومات الالكترونية، معاً نحو تعامل رقمي امن، سلطنة عمان, 2005.
8. تدابير مكافحة الجرائم المتصلة بالحواسيب، مؤتمر الامم المتحدة الحادي عشر لمنع الجريمة والعدالة الاجتماعية، بانكوك, 2005.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98

9. إبراهيم الدسوقي أبو الليل، الجوانب القانونية للتعامل عبر وسائل الاتصال الحديثة، مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، المجلد الثالث, 2004.
10. بعجي احمد، تطور مفهوم حماية الحق في الخصوصية، بحث منشور، مجلة القانون والمجتمع، ال عدد1, المجلد الثامن، الجزائر,2020.
11. شيماء عبد الغني عطاء الله، تراجع الحق في الخصوصية في مواجهة الإتصالات الإلكترونية، مجلة كلية القانون الكويتية العالمية، العدد 10, السنة الثالثة، يونيو 2015.
12. منى تركي الموسوي، جان سيريل فضل الله، الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية الجامعة , 2013.
13. مريم نباش، التجسس وانتهاك حق الخصوصية في العالم الرقمي (دراسة وصفية تحليلية لبرنامج بيغاسوس)، بحث منشور، مجلة الدراسات الاعلامية والاتصالية، جامعة الجزائر، كلية القانون، مجلد (٢) العدد (٣)، ٢٠٢٢.
14. فتحية حزام، الحق في الحياة الخاصة في البيئة الرقمية، بحث منشور، مجلة الدراسات القانونية المقارنة، جامعة محمد بوقرة، كلية القانون، الجزائر، مجلد (٨) العدد (١)، ٢٠٢٢.

**خامساً: القرارات**

1. قرار الجمعية العامة للأمم المتحدة سنة 2014، رقم (167/68) بتاريخ 19 نوفمبر 2014 في الدورة التاسعة والستين.
2. قرار الامم المتحدة رقم (167/68) بتاريخ ١٨ تشرين الأول لسنة ٢٠١٣ , الدورة ٦٨ البند ٦٩ (ب) /A/RES/73/16
3. قرار الامم المتحدة رقم (167/68) بتاريخ ١٨ تشرين الأول لسنة ٢٠١٣ , الدورة ٦٨ البند ٦٩ (ب) /A/RES/73/16
4. قرار الامم المتحدة رقم (٦٩ / ١٦٦) بتاريخ ١٨ كانون الأول 2014, الدورة ٦٩، البند (٦٨ (ب) /A/RES/73/16.

**سادساً: الاعلانات والمواثيق**

1. اتفاقية الامم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000.
2. اتفاقية بودابست لسنة 2001 المتعلقة بمكافحة الإجرام المعلوماتي.
3. الاعلان العالمي لحقوق الانسان لسنة 1948.

العهد الدولي الخاص بالحقوق المدنية والسياسية لسنة 1966.


Licensed under Creative Commons Attribution 4.0 International License (CC BY 4.0)
https://doi.org/10.64002/63tzss98