الحماية القانونية للحق في الخصوصية المعلوماتية

(دراسة مقارنة)

مشروع رسالة مقدم استكمالاً لمتطلبات الحصول على درجة الماجستير في تخصص الأنظمة

اعداد الطالبة :

رؤى سعد القرني

جامعة الملك عبد العزيز

المملكة العربية السعودية

الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)

رؤى سعد القرني
قسم القانون – جامعة الملك عبد العزيز – المملكة العربية السعودية
البريد الإلكتروني :Roaa.alkarni@hotmail.com

الملخص :

يعد الحق في الخصوصية احدى أهم الحقوق الأساسية للإنسان، حيث إنه يرتبط بشكل رئيسي بكرامة الانسان واحترامه. ومن هذا المنطلق، عملت التشريعات والقوانين على مدار السنين على حماية حق الفرد في حرية الانفراد بنفسه وعدم أحقية الاخرين في التدخل في شؤونه الخاصة الا بإذنه. الا ان التطور التقني السريع للعديد من جوانب حياة الفرد وأهمها الجانب الاجتماعي، من حيث طرق التواصل الجديدة بين الأفراد، وبين الأفراد والجهات الرسمية، وبين الفرد والمجتمع التي تتضمن الكشف عن نسبة من هذه الخصوصية مقابل الخدمات المقدمة بالمقابل. مما خلق مفهوم الخصوصية المعلوماتية الذي يتعمق هذا البحث في دراسته كمفهوم قانوني جديد وما يتطلبه من حماية خاصة على الصعيد الوطني والدولي. ويتضمن الجزء الأول الخط الزمني لمفهوم الخصوصية المعلوماتية والتحديات التي تواجه توفير الحماية لها. ويدرس الجزء الثاني الجوانب الأساسية المتعلقة بالخصوصية المعلوماتية من خصائص وأمثلة وتحديات، والجهود الدولية ومساهمتها في التعزيز من حماية هذا الحق ونشر الوعي عنه. ويناقش الجزء الثالث التحديات القانونية التي تواجه الحماية الدولية للحق في الخصوصية المعلوماتية مع ذكر الموقف القانوني المعاصر تجاه هذا الحق. ويستنتج البحث مدى كفاية وفعالية الحماية الدولية المتاحة للحق في الخصوصية المعلوماتية بهدف بيان نقاط الضعف والقوة والمساهمة في تطوير الكيان القانوني الدولي لحماية الخصوصية المعلوماتية.

الكلمات المفتاحية: الحماية القانونية – الحق – الخصوصية المعلوماتية – الجهود الدولية – البيانات الشخصية.

The Legal Protection of Personal Data privacy (A Comparative Study)

Saad Al-Qarni's visions
Law Department - King Abdulaziz University - Kingdom of Saudi Arabia
Email: Roaa.alkarni@hotmail.com

Abstract:
The right to privacy is one of the basic human right, as it mainly relates to human dignity and respect. From this point on, legislation and laws have worked over the years to protect the right of the individual to freedom of his own and the inability of others to interfere in his private affairs without his permission. The rapid technical development has evolved in all aspects of the individual life, most importantly of which is the social aspect, in terms of new ways of communication between individuals, between individuals and official bodies, and between individuals and society, which includes revealing a percentage of this privacy in exchange for the services provided in return. Which created the concept of data privacy, which this research delves into in its study as a new legal concept and what it requires of special protection at the national and international levels. The first chapter includes the timeline of the concept of data privacy and the challenges facing providing protection for it. The second chapter studies the basic aspects related to data privacy, including characteristics, examples, challenges, and international efforts and their contribution to strengthening the protection of this right and spreading awareness about it. The third chapter discusses the legal challenges facing the international protection of the right to data privacy with a mention of the contemporary position of the Kingdom of Saudi Arabia and comparative countries towards this right. The research concludes the adequacy and effectiveness of the international protection available for the right to data privacy with the aim of showing weaknesses and strengths in contribution to the development of the international legal entity to protect data privacy.

Keywords: Legal Protection - The Right - Information Privacy - International Efforts - Personal Data.

المقدمة

إن التطور التقني السريع الذي تشهده الدول عامةً ساهم في بروز العديد من التحديات على الصعيد الثقافي والاقتصادي وبالأخص الشخصي. وحيث إن أغلب منصات التقنية الحديثة تقوم على تبادل وحيازة البيانات المعلوماتية المتعلقة بالأفراد ونشاطهم وتساهم في تيسير نقل المعلومات بين الأفراد من خلال تطبيقات وسائل التواصل الاجتماعي. وتساهم منصات التقنية الحديثة كذلك في تحويل تبادل البيانات وحفظها من الشكل التقليدي إلى الشكل المعاصر الذي يتمثل في نشاطات عدة أبرزها: المراسلة الالكترونية عبر وسائل التواصل الاجتماعي أو حفظ البيانات الشخصية في منصة لجمع المعلومات وحفظها من التلف الورقي أو الضياع. إلا ان هذه النقلة في تبادل المعلومات وحفظها ترتب عليها تهديد جديد بالاعتداء على حق الخصوصية المعلوماتية من خلال اختراق الحسابات الخاصة وسرقة بياناتها والتشهير بها مما قد يترتب عليه آثار متعددة على الشخص من تشويه لسمعته الشخصية أو تعريضه للمساءلة القانونية أو انتهاك لحرمته وحرمة أسرته. وحيث إنه لا خلاف في أن الحق في الخصوصية يعد من الحقوق الدستورية الأساسية واللازمة للإنسان بغض النظر عن وجود الأنظمة واللوائح الحكومية لارتباطه بكرامة الإنسان وكيانه.

وعليه يلعب ارتباط الخصوصية بكرامة الإنسان دوراً مهماً في استقرار المجتمعات وتحقيق التقدم الحضاري، في الوقت الذي تحرص فيه المجتمعات الدولية والديموقراطية جاهدةً على حماية هذا الحق وكفالته والتأكد من وضع السياسات التي تؤكد على أهميته نظراً لما يشكل انتهاكه من تدمير لكرامة وكيان الفرد.

ويمكن القول أن تطور الوسائل التقنية المعلوماتية يضع الخصوصية في موضع حساس أكثر عرضةً للانتهاك والاستغلال لذلك تقوم المسؤولية على عاتق الدول والهيئات والمنظمات المختصة في وضع الضمانات والسياسات

القانونية التي تجابه الخطر الواقع على الحق في الخصوصية المعلوماتية في ظل التطور المستمر لوسائل التقنية.

أهمية الدراسة:

تكمن أهمية الدراسة في تحفيز الكيان القانوني على مجاراة التطور التقني الذي يهدد الحق في الخصوصية المعلوماتية من خلال سن السياسات والأنظمة التي تكفل هذا الحق وتعزز من أهميته لدى المجتمعات، وتحد من سلطة شركات التقنية في حيازة واستخدام البيانات الشخصية للأفراد. إضافة الى نشر التوعية حول حماية البيانات المعلوماتية من قبل الانتهاكات الصادرة من الأفراد او الشركات ومدى أحقية الشركات التقنية في استحواذ واستخدام البيانات الشخصية للفرد. تتمثل الأهمية العلمية للدراسة في الاثراء القانوني حول الحق في الخصوصية المعلوماتية ونشر الوعي حول أهمية هذا الحق ومدى تأثير انتهاكه على كرامة الفرد وكيانه. وتتمثل الأهمية العملية لهذه الدراسة في توجيه المجتمع التقني من خلال الانظمة القانونية لمراعاة واحترام الحق في الخصوصية المعلوماتية عند تأسيس وخلق برامج التقنية الجديدة.

مشكلة الدراسة:

تكمن مشكلة الدراسة في تفاقم الاعتداءات على الحق في الخصوصية المعلوماتية عبر وسائل التقنية واستمرار التحدي حول مجاراة التطور المستمر لهذه التقنيات من قبل المجتمع الدولي القانوني. يعد الاعتداء على الحق في الخصوصية احدى أبرز المشاكل التي تواجه مستخدمي التقنية الحديثة نظراً لاستمرار تداخل وانسجام التقنيات الحديثة مع حياة الفرد وأنشطته اليومية. حيث إن عدم وضوح نطاق الحماية الدولي للبيانات الشخصية يترتب عليه استمرار الشركات التقنية في الاعتداء على حق الخصوصية للمستخدمين فنتبين في هذه الدراسة أهم الوسائل المجابهة لضمان هذا الحق وتعزيز الانظمة القانونية التي تساهم في حمايته.

تساؤلات الدراسة:

يتفرع من مشكلة الدراسة تساؤلات سيتم الإجابة عنها خلال الدراسة وهي:

١ . ما هو مفهوم الحق في الخصوصية من المنظور التاريخي ومنظور الفقه الاسلامي؟

٢ . ما هي التحديات التي تواجه الخصوصية المعلوماتية عبر وسائل التقنية؟

٣ – ما مدى فعالية الجهود الدولية الحالية في مجابهة اعتداءات الخصوصية المعلوماتية؟

٤ – ما مدى الزامية الضمانات القانونية لحق الخصوصية المعلوماتية وآلية تنفيذها؟

أهداف الدراسة:

تهدف هذه الدراسة إلى ما يلي:

١. ايضاح مفهوم الحق في الخصوصية المعلوماتية والحقوق التي يترتب عليها.

٢. بيان الأخطار التي تترتب على عدم حماية البيانات الشخصية للمستخدمين عبر وسائل التقنية.

٣. تسليط الضوء على مدى فعالية الجهود الدولية في حماية الخصوصية المعلوماتية.

٤. بيان مدى الزامية الضمانات القانونية في حماية الحق في الخصوصية المعلوماتية.

الدراسات السابقة:

الدراسة الأولى: حق الخصوصية في الفقه الإسلامي

إعداد: إبراهيم بن سلمان بن عبد الله الشايع، اشراف الدكتور زيد بن عبد الكريم الزيد، رسالة ماجستير، المعهد العالي للقضاء، جامعة الامام محمد بن سعود الإسلامية، الرياض، ٢٠٠٦

تبين هذه الدراسة ما جاءت به الشريعة الإسلامية من أصول تحفظ وتصون حقوق الفرد في عبارات جامعة وسهلة، مما سهلت بذلك تكييف هذه

الأصول بما يناسب التغيرات والتحديات التي تهدد هذه الحقوق. ومن هذه الحقوق الحق في الخصوصية، نظراً بأنه أصبح له أوجه متعددة كالخصوصية المعلوماتية فأصبح مطلبا مستحدثاً يتطلب بيان موقف الشريعة منه كما توضح هذه الدراسة. وتكمن أوجه الشبه بين الدراسة السابقة مع الدراسة الحالية في أهمية بيان عناية الشريعة الإسلامية في حماية الحق في الخصوصية. وتختلف الدراسة السابقة مع الدراسة الحالية في ان الدراسة الحالية متخصصة في حماية الخصوصية المعلوماتية.

الدراسة الثانية: حماية الخصوصية الشخصية لمستخدمي مواقع التواصل الاجتماعي

اعداد: القحطاني، محمد بن عيد عبد الهادي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية، قسم الشريعة والقانون، ٢٠١٥.

تتطرق هذه الدراسة الى بيان طبيعة مواقع التواصل الاجتماعي التي تفرض نوعاً خاصاً من التواصل ومشاركة المعلومات مع الأصدقاء والأهل، مما يطرح العديد من التساؤلات حول مدى احقية المستخدمين في السماح بوصول بياناتهم الشخصية للأخرين، وحق المستخدمين في الوصول الى تلك البيانات وتصحيحها وطبيعة البيانات التي تتوجب الحماية القانونية. وتناقش الدراسة مدى كفاية الحماية القانونية الموجودة في العالم العربي والمملكة العربية السعودية. وتتمثل أوجه الشبه في ان الدراسة السابقة تتفق مع الدراسة الحالية في تناول موضوع مدى الحماية المتوفرة لحماية حق الخصوصية لمستخدمي وسائل التواصل الاجتماعي. وتختلف الدراسة السابقة مع الدراسة الحالية في ان الدراسة السابقة تنحصر في بيان مدى حماية الخصوصية وطرق تصدي انتهاكها على الصعيد الوطني، بينما الدراسة الحالية تتناول فعالية الجهود الدولية والتشريعات القانونية في حماية حق الخصوصية لبقية الدول.

الدراسة الثالثة: الحماية الجزائية للحق في الحياة الخاصة بمواجهة وسائط الاتصال الالكتروني: دراسة مقارنة

اعداد: أمل منير بركات الشواورة، اشراف الدكتور ممدوح حسن العدوان، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، عمان، ٢٠١٨.

تقوم هذه الدراسة على بيان الحماية الجزائية للحق في الحياة الخاصة بعد ظهور الوسائل الالكترونية التي أصبحت تعرض حياة وخصوصية الأفراد للانتهاك. لذا تتناول الدراسة تحليل النصوص الموضوعية والاجرائية المعنية بتوفير الحماية لخصوصية الأفراد، إضافة الى دراسة دور قوانين الجرائم الالكترونية وقياس مدى كفايتها في مواجهة هذه الاعتداءات. تكمن أوجه الشبه في اتفاق الدراسة السابقة مع الدراسة الحالية في تناول أهمية مواكبة القانون للتطور التقني الذي يهدد حرمة الحياة الخاصة للأفراد. وتختلف الدراسة السابقة عن الدراسة الحالية في إن الدراسة الحالية تركز على الجهود الحماية الدولية للخصوصية المعلوماتية بينما الدراسة السابقة مقتصرة على جهود المشرع الأردني في حماية حق الحياة الخاصة.

منهج الدراسة:

تتبع هذه الدراسة المنهج التحليلي المقارن كمنهج أساسي للدراسة وستتم المقارنة بين التشريعات القانونية الخاصة بحماية الحق في الخصوصية المعلوماتية في بعض الدول من ناحية وعلاقتها بالاتفاقيات الدولية حول حماية الحق في الخصوصية المعلوماتية من ناحية أخرى. وسيتم وفقا لذلك تحليل الاتفاقيات والنصوص المبرمة في حماية هذا الحق والسياسات التي تقوم عليها المنصات التقنية في جمع البيانات والمعلومات الشخصية. كما سيتم استخدم المنهج التاريخي في بداية الدراسة لاستعراض الخلفية التاريخية ونشأة الحق في الخصوصية.

تقسيم البحث:

- **المبحث التمهيدي:** أثر التقنية في خصوصية الأفراد والضمانات القانونية التي تحميها
- **المبحث الأول:** دور التقنية الحديثة في حياة الأفراد

-**المطلب الأول:** دور منصات وسائل التواصل الحديثة وتوجهاتها حول خصوصية الأفراد

١)**الفرع الأول:** مفهوم الخصوصية المعلوماتية

٢)**الفرع الثاني:** مخاطر الإفصاح عن الخصوصية ودرجاتها

-**المطلب الثاني:** امثلة على اشكال الانتهاكات والجرائم الالكترونية المهددة لحق الخصوصية المعلوماتية

١)**الفرع الأول:** نشأة ومراحل تطور الجرائم الالكترونية وأنواعها

- **المبحث الثاني:** الجهود الدولية في حماية الحق في الخصوصية المعلوماتية

-**المطلب الأول:** دور الاتفاقيات والمعاهدات الدولية في تعزيز وتأكيد مبدأ حماية الخصوصية المعلوماتية للأفراد

-**المطلب الثاني:** الموقف الدولي المعاصر حول أهمية حفظ الحق في الخصوصية المعلوماتية

١)**الفرع الأول:** دور المنظمات الدولية في تحقيق التعاون الدولي

٢)**الفرع الثاني:** الموقف القانوني الدولي حول أهمية حفظ الحق في الخصوصية المعلوماتية

تمهيد

أثر التقنية في خصوصية الأفراد والضمانات القانونية التي تحميها

يلاحظ في الآونة الأخيرة أن وسائل التقنية الحديثة تطورت من كونها وسائل مساعدة وثانوية للفرد الى وسائل أساسية وبل بديلة عن الفرد في بعض الأحيان. مما يوجب أعادة النظر حول مدى خطورة الجانب السلبي لهذه الوسائل وتهديدها لحقوق الإنسان ومن أهمها حقه في الخصوصية.

وعليه باتت الأنظمة المعلوماتية واحدة من أكثر الوسائل شيوعاً، لما تقدمه للمؤسسات والشركات وغيرها من المراكز الحكومية أو الخاصة في تنظيم الكم الهائل من المعلومات المتعلقة بطبيعة عمل تلك المؤسسات والشركات وتخزينه ومعالجته ونقله. مما أثيرت عدة تساؤلات حول مدى إمكانية هذه المؤسسات والشركات في الوصول الى المعلومات الشخصية للفرد، وطبيعة المعلومات التي يتم جمعها وما هو الأثر المترتب جراء ذلك على خصوصية الأفراد.

ولبيان الأثر الحقيقي للتنقية الحديثة على خصوصية الأفراد، يلزم أن نأخذ بعين الاعتبار التطور التاريخي لمفهوم الخصوصية وما يشمله من تغيرات ومؤثرات اجتماعية وقيمية. وأثر هذا المفهوم العصري للخصوصية على تحديد نطاق حماية هذا الحق واحترامه. حيث إن قديماً، كان نطاق المعلومات الشخصية للفرد لا يتعدى نطاقه العائلي الخاص، بينما في عصرنا الحالي، أصبح النطاق المعلوماتي أوسعاً ثلاثة أضعاف ما كان عليه، نتيجة اتساع نطاق الاستخدام للوسائل التقنية المتعددة لجميع أفراد المجتمع. إلا أن هذا الاتساع ساهم في تصاعد عدد من الجرائم المهددة لخصوصية الفرد ومنها التجسس الالكتروني، الاختراق وسرقة البيانات الشخصية وغيرها العديد من الجرائم الالكترونية التي تستمر بالظهور مع تطور واتساع النطاق التقني لهذه الوسائل الحديثة. وفي هذا الفصل، سيناقش الباحث دور وأثر التقنية الحديثة في انتهاك مبدأ الحياة الخاصة والخصوصية المعلوماتية للأفراد. وسيتطرق هذا الفصل الى مناقشة دور التقنية الحديثة في حياة الأفراد وعلاقتها بالتحديات

المهددة لخصوصية الأفراد المعلوماتية وهذا في المبحث الأول. بينما يتناول المبحث الثاني الجهود الدولية في توفير الحماية للحق في الخصوصية المعلوماتية من خلال معاينة دور المنظمات الدولية ومدى فعالية تطبيق الاتفاقيات المبرمة من قبلها في تحقيق التعاون الدولي تجاه حماية هذا الحق.

المبحث الأول: دور التقنية الحديثة في حياة الأفراد

على الرغم من سلبية أغلبية سياق الحديث حول أثر التقنية الحديثة في خصوصية حياة الفرد إلا أنه من الجدير رسم صورة حيادية تظهر كلاً من الجوانب السلبية والايجابية. لما قدمته التقنية الحديثة من دور عظيم في رفع مستوى المعيشة للفرد وتسهيل العمليات الحكومية والدولية في شتى مجالات البشرية. نظراً لما تقوم عليه أغلبية وسائل التقنية الحديثة من نظم معلوماتية واتصالية، ترتب عليها انسياب دولي للمعلومات وتطور مفهومي لحرمة الحياة الخاصة للفرد، أي يحق لأي مستخدم أن يحافظ على سرية معلوماته الشخصية وما يتعلق بذلك من خطوات مصاحبة. حيث إن جمع البيانات في هذه النظم المعلوماتية يساهم في تيسير إدارة الدولة لشؤون افرادها عبر المواقع الحكومية الرئيسية التي تقدم للدولة الوسائل الفعالة من تحليل واسترجاع للبيانات خلال تنظيم عملها.

•الجانب الايجابي للتقنية في حياة الأفراد

ويتمثل الجانب الايجابي للتقنية في حياة الأفراد في الخدمات المقدمة للتواصل السريع بين الأفراد وبين الأفراد والجهات الحكومية أو الشركات الخاصة. وينتج عن هذه السهولة في التواصل وتبادل المعلومات في تيسير العديد من الامور للفرد مثل تجنب العديد من المصاعب التي كانت تصاحب التواصل بالطرق التقليدية، مثل السفر مسافات طويلة أو الانتظار لأيام أو شهور حتى تصل رسائلهم عبر البريد، إلى جانب مساهمة هذا النوع من التقدم التكنولوجي في طريقٍ ميسر وآمن للأفراد وصولاً إلى الاحتفاظ بمعلوماتهم الشخصية كبديل عن الطرق التقليدية لحفظ هذه المعلومات وما

تعتريه تلك الطرق من مخاوف مرتبطة بالتلف أو الضياع، فقد أصبح ممكنا أن يتم حفظ هذه المعلومات بطريقة إلكترونية تتميز بسهولة الحفظ وسرعة الرجوع إلى المعلومات في أي وقت ومن أي مكان مع هامش بسيط لتعرضها للتلف أو الضياع"[1] إذ أن منصات التقنية الحديثة قدمت للفرد حماية أكثر من احتمالات كثيرة ومنها التلف والضياع أو السرقة بعكس الرسائل الإلكترونية التي تحتمل مخاطر أقل من هذه الناحية.

من ناحية موضوعية أكثر، فإن دور التقنية الحديثة لا يقتصر على التطور من ناحية التقنية لطرق التواصل التقليدية بل أيضاً من ناحية موضوعية متعلقة بتوفير الفرص للفرد بأن يعبر عن ذاته وآرائه بطرق مختلفة وسهلة وأقل تكلفة. حيث إن منصات التواصل الاجتماعي وأشهرها الفيس بوك، قدمت شكلاً حديثاً للتواصل البشري وجمع المعلومات واستخدامات التقنية لعدة خدمات شخصية كنشر الآراء والتعليقات الشخصية أو كتابة المقالات وتبادل الخبرات بين الأفراد. مما ساهم في تعزيز أحد الحقوق الأساسية الإنسانية وهو الحق في التعبير عن الرأي بين أفراد المجتمع، مع الأخذ بعين الاعتبار الضوابط الأخلاقية والإنسانية. ونستنتج مما ذكر أعلاه، أن دور التقنية الحديثة في حياة الفرد تساهم في تعزيز عدة حقوق إنسانية رئيسية من خلال الخدمات التي توفرها للفرد من جانب، وتعرض ذات الحقوق لتهديد الانتهاك من جانب آخر، كخطر التعدي على حرية التعبير والرأي وخطر انتهاك حق الحياة الخاصة. حيث إن الإعلان العالمي لحقوق الإنسان يعزز من أهمية حماية هذين الحقين في المادة الثانية عشر والمادة التاسعة عشر. وعلى الرغم من أن وسائل التقنية الحديثة ساهمت في توفير منصة للتعبير ومشاركة المعلومات وقامت بتوفير حماية محدودة لخصوصية الأفراد، إلا أنها في ذات الوقت ساهمت في ظهور عدة تحديات أخرى تهدد حق الفرد في الخصوصية مثل

١ رزق، سلمودي وآخرون (٢٠١٧م). **الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي**. مجلة الجامعة العربية الأمريكية للبحوث، مجلد ٣، العدد ٢، ص٢.

الاختراق الالكتروني أو انتحال الشخصية وسرقة البيانات الشخصية. وهذا ما سيتطرق له المطلب الأول من هذا المبحث بشكل تفصيلي.

•الجانب السلبي للتقنية في حياة الأفراد

على الرغم من الجوانب الايجابية المذكورة أعلاه، الا أن تطور الوسائل الحديثة للتقنية أتاح فرصاً أوسع للوصول الى بيانات الأفراد الشخصية وانتهاكها. فعلى سبيل المثال، أصبح من السهل على الجهات الوطنية الرسمية مراقبة مواطنيها وجمع عدد كبير من البيانات التي تخصهم، مما أثار الجدل حول معيار ومدى أحقية هذه الجهات في الوصول الى البيانات الخاصة بالأفراد واستعمالها من غير اذن مسبق بهدف حماية المصلحة العامة على سبيل المثال. حيث إن الأحقية في الوصول الى هذه البيانات وجمعها قد يكون مبني على مبرر قانوني سليم، الا أن النقص في التشريعات التنظيمية لهذه الجهات المعنية بجمع البيانات قد يؤدي الى التطرف في ممارسة هذه الأحقية.

المطلب الأول: دور منصات وسائل التواصل الحديثة وتوجهاتها حول خصوصية الأفراد

أحدثت وسائل التواصل الحديثة نقلة نوعية في طبيعة التواصل بين الأفراد، حيث إن معطيات التواصل البشري التقليدي اختلف بدرجة كبيرة عن طبيعة التواصل الالكتروني الذي يفتقر الى العديد من الخصائص التي يتميز بها التواصل على الطريقة التقليدية. حيث إن التواصل الالكتروني قد سهل للعديد من الأفراد ممن يواجهون صعوبات في بناء العلاقات على أرض الواقع بأن يلجأوا للعالم الافتراضي لتوسيع شبكة معارفهم. حيث إن شبكات التواصل الاجتماعي تتميز بخصائص عدة تخدم الانطوائيين من الأفراد، كخاصية غياب لغة الجسد والقدرة على إخفاء الهوية وبناء هوية مثالية ووهمية تخفي الكثير من العيوب التي تلاحقهم في الحياة الحقيقية[1]. لذا سيتطرق هذا المطلب

1 Schlosser, Ann E. (2020). **"Self-disclosure versus self-presentation on social media"**. Current Opinion in Psychology, Volume 31, P1-6

بالذات الى تسليط الضوء على العلاقة التي تجمع المستخدمين بمواقع التواصل الاجتماعي المختلفة، وأثر ذلك على مستوى الخصوصية المتبع هناك، والخطوات التي تتبعها هذه المواقع لاحترام خصوصية المستخدمين وتجنب انتهاكها، وصولاً إلى التطرق لمحاولات الدول الحد من خطورة الجرائم الناجمة عن سياسات الخصوصية في الاعلام الجديد.

أولاً، يتوجب أن ننص على مفهوم الخصوصية وفقاً لسياسات منصات التواصل الاجتماعي وما يترتب على هذا المفهوم من أثر حول مفهوم الخصوصية التقليدي. ويعرف بالين ودوريش ٢٠١٤، الخصوصية في منصات التواصل الاجتماعي بأنها الإدارة المستمرة للحدود الشخصية في مختلف المجالات، وإدارة درجة الكشف عن المعلومات الشخصية داخل تلك المجالات. حيث إن ممارسة الخصوصية في مواقع التواصل الاجتماعي تختلف من فرد لآخر بحسب عوامل عدة مثل البيئة المادية المحلية، وطبيعة الجمهور، والوضع الاجتماعي، والهدف، إلى جانب الدافع أو النية.[1] إضافة الى اختلاف مواقع التواصل الاجتماعي من حيث طبيعة مشاركة المعلومات ودرجة الكشف عن المعلومات الشخصية للفرد. ويُنظر إلى الخصوصية في مواقع التواصل الاجتماعي وفقاً لبعض الآراء على أنها عملية تقييد الوصول إلى المعلومات الشخصية للمستخدمين، وهو أمر يتنافى مع فكرة تواجد مواقع التواصل الاجتماعي التي تتطلب مشاركة الناس معلوماتهم ويومياتهم، والكتابة بصورة أكبر عن أنفسهم وحياتهم الخاصة، مما يخلق حالة من التناقض بين العالمين الواقعي والافتراضي، حيث يلجأ الأفراد إلى رفض الحديث عن حياتهم

1 Marwick, Alice E. & Boyd, Danah. (2014) "**Networked privacy: How teenagers negotiate context in social media**" new media & society, Vol. 16(7) 1051–1067.

الشخصية في العالم الحقيقي، بالتزامن مع كشفهم الكثير من المعلومات والخصوصيات عبر الواقع الافتراضي[١].

الفرع الأول: مفهوم الخصوصية المعلوماتية

نظراً للتحول الكبير لطبيعة التواصل بين الأفراد نتيجة التقدم التقني الذي قدم طرق جديدة للتواصل ومشاركة المعلومات من خلال شبكة معلوماتية أسهمت في تيسير وسرعة تبادل المعلومات بين الأفراد والشركات وحتى الدول. تفرع من مفهوم الحق في الخصوصية، مفهوم الخصوصية المعلوماتية وهي تعد إحدى أنواع الحق في الخصوصية أو الحق في حرمة الحياة الخاصة وتعرف بأنها حق الفرد في العيش بالطريقة التي تروق له والحفاظ على سرية الحياة الخاصة به، من غير أن يتدخل آخرون في ذلك[٢]. إلا أن هذه النقلة ذاتها بمحاسنها ساهمت في تيسير الوصول الى البيانات الشخصية للأفراد مما يعرضها لاحتمالية الانتهاك والسرقة وانتحال الشخصية وانتهاك خصوصية الأشخاص. امتداداً من ذلك، كان ولابد من وضع حدود وقواعد منظمة لمنصات معالجة البيانات لحماية حقوق الفرد المهددة في منصات التقنية كحق الخصوصية الذي ينتهك بعدة طرق منها الاطلاع على بيانات خاصة بدون إذن، التشهير والسرقة. لذلك تنفرد الخصوصية المعلوماتية عن مفهوم الخصوصية العام نتيجةً لاختلاف خصائصها والتحديات التي تواجه الفرد عند انتهاكها.

ويعرف مصطفى ٢٠١٦ الخصوصية المعلوماتية بأنها "حق الشخص في أن يتحكم بالمعلومات التي تخصه"[٣]، كما يعرف الفقيه الأمريكي الآن ويستن الخصوصية المعلوماتية بأنها "القدرة على التحكم في مقدار ما نكشفه

---

1 Ibid.

٢عودة، سلمان (٢٠١٧) **الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة**، مجلة آثار الرافدين، كلية الرافدين الجامعة – قسم القانون، المجلد ١، العدد ٢٩، ص٤.

٣عائشة، مصطفى. (٢٠١٦). "**الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية**". مجلة الفقه والقانون. المجلد ٢، العدد ٦، ص٧٤.

عن أنفسنا للآخرين" حيث كان الآن ويستن من أوائل الباحثين القانونيين الذين وضعوا الأساس لقانون الخصوصية في كتابه الصادر عام ١٩٦٧م بعنوان "الخصوصية والحرية" استكمالاً للأسس القائمة حول التعريف بحق الخصوصية كحق قانوني من قبل قاضي المحكمة العليا للولايات المتحدة لويس براندیس أواخر القرن التاسع عشر. وتبعه الآن ويستن في القرن العشرين في استكمال مفهومه للحق في الخصوصية. حيث إن مفهوم الحق في الخصوصية قديماً كان يتمحور حول الحد من سيطرة الحكومة على الاستقلال الجسدي للأفراد، لكن مع موجة التطور التقني، تصاعدت التحديات التي تواجه خصوصية الأفراد وتغير مفهوم الخصوصية بناء على ذلك.[١]

ويسعى ميلر ١٩٧١م في كتابه بعنوان "الاعتداء على الخصوصية: أجهزة الكمبيوتر وبنوك البيانات والملفات" في المساهمة بشكل بارز في مجال حماية الخصوصية، بعيداً عن التعميمات والأفكار المبتذلة المليئة بالعاطفة والبعيدة عن المنطق فيما يخص التعامل مع الحق في الخصوصية.[٢] ويوضح المؤلف جوزيسفون ١٩٧١م أن رؤية ميلر حول التحكم في استخدام المعلومات الخاصة كانت كالآتي "تدور قوانينه المتعلقة باستخدام البيانات حول الافتراض بأن المعلومات الشخصية المسلمة لغرض معين ولجمهور معين (كبيانات الائتمان الممنوحة للبنك لأغراض الحصول على قرض) لا ينبغي استخدامها لأي غرض آخر أو رؤيتها من قبل أي شخص آخر.[٣]

وعلى الرغم من اختلاف التعريفات لحق الخصوصية المعلوماتية بين هؤلاء الفقهاء إلا أن النقاط المشتركة بينهم تتمثل في السعي وراء الحد من السلطة الممنوحة للحكومات أو الأفراد خاصة فيما يتعلق بعملية الاطلاع على

1 Rollenhagen, Luisa. (2021). **"Alan Westin is the father of data privacy law"**. https://www.osano.com/articles/alan-westin

2 Josephson, Michael S. (1971). **"Miller: The Assult on Privacy"**. Michigan Law Review, Vol 69, Iss 7 , P 1389.

3 *Ibid*, p1390.

البيانات الشخصية للأفراد واستعمالها بغض النظر عن الأسباب، مع تسليط الضوء على النقص التشريعي القانوني حول حماية الأفراد من الانتهاك الشخصي الالكتروني ومن مخاطر التقنية بشكل عام. وتختم مصطفى ٢٠١٦ في مقالها حول خصوصية المعلومات، بأن المصطلح يرتبط بشكل جوهري مع حماية البيانات حيث إن جوهر خصوصية الفرد يتمثل في البيانات والمعلومات التي تكشف عن هويته وحياته الخاصة وحالته الصحية أو الإجتماعية الخ، لذلك انتهاكها يعد انتهاكاً مباشر لهوية الشخص وسمعته وحرمة حياته الخاصة. وتقع كل من خصوصية الفرد المعلوماتية وحقه في الحياة الخاصة تحت المظلة الكبرى للحق في الخصوصية كحق انساني جوهري.[١]

وبحسب مواقع التواصل الاجتماعي، نستنتج أن مفهوم الخصوصية المعلوماتية يختلف عن مفهوم الخصوصية التقليدي خارج نطاق مواقع التواصل الاجتماعي. حيث إن معيار التواصل بين الأفراد خلال مواقع التواصل يقوم على فكرة أساسية مفادها زيادة حجم الاتصال والانفتاح بين الأفراد، مع منح كافة المستخدمين فرصاً متساوية للتفاعل والمشاركة، مما زاد من مستوى الإفصاح عن الخصوصية بين صفحاتها الإلكترونية، وهو أمر يؤكده موقع " فيس بوك "الشهير عبر بيانه التأسيسي الذي يقول: " نعمل على أن نساهم في بناء عالمٍ أكثر انفتاحاً واتصالاً"[٢]. بينما التواصل بين الأفراد في الحياة الواقعية يكون أكثر تحفظاً بالعادة واقل انفتاحاً من حيث درجة مشاركة المعلومات الشخصية، خصوصاً في اللقاءات الأولى. على سبيل المثال، فيس بوك يعد من أكثر المواقع الاجتماعية انتشاراً في العالم وأكثرها عمقا في عالم تجميع المعلومات الشخصية. حيث إن البيانات التي يشجع فيسبوك مستخدميه

١ عائشة، مصطفى، **مرجع سابق**، ص٧٥.

2 Xie, Wenjing. & Kang, Cheeyoun. (2015). **See you, see me: Teenagers' self-disclosure and regret of posting on social network site**, Computers in Human Behavior, Vol 52, p399.

مشاركتها تشمل الآتي: الآراء والخلفيات الفكرية الشخصية، الأشخاص المشهورة المهتم بها من قبل المستخدم وغيرها العديد من المعلومات الشخصية والاهتمامات التي تظهر سلوك الشخص وتوجهاته تجاه مسائل مهمة في الحياة.[1]

ويمكن القول أن التطور التقني الذي شهدته مواقع التواصل الاجتماعي عمل على زيادة العمق المعلوماتي للبيانات الشخصية للأفراد، والمتاحة لشركات مواقع التواصل الاجتماعي من خلال القوالب التي صنعوها للمستخدمين، الأمر الذي زاد من عمليات محاولة السيطرة على البيانات وانتهاك الخصوصية المعلوماتية للأفراد، حيث إن أكبر عامل مؤثر في هيكلة هذه القوالب هو سياسة الخصوصية، وهو عبارة عن بيان أو مستند قانوني يكشف عن بعض أو كل الطرق التي يقوم بها الطرف الثالث بجمع، واستخدام، وكشف وإدارة بيانات العميل او المستخدم.[2] حيث إن سياسات الخصوصية لأكثر المواقع الاجتماعية استخداماً تشمل بنود تتعدى بشكل صريح على خصوصية الفرد. ويعود ذلك إلى عدة عوامل أبرزها عدم كفاية الضمانات ضد الشركات المشاركة في جمع البيانات، قلة الإشراف من قبل فيسبوك على مطورين الموقع، واخيراً البنود والشروط الطويلة والواسعة المعنى التي يقبلها العديد من المستخدمين بغير علم.

وشهدت الأعوام الأخيرة تضاعفاً ملحوظاً في أعداد مستخدمي مواقع التواصل الاجتماعي المختلفة، الذين كسروا حاجز الـ ٢ مليار مستخدم، يقومون سوية بتحميل ومشاركة مئات المليارات من البيانات والمعلومات الشخصية، وسط توقعات بمزيد من النمو تعيشه هذه الأرقام خلال السنوات

---

١ الزهراني، يحيى بن مفرح. (٢٠١٣). "**تحديات الأمن المعلوماتي في الشبكات الاجتماعية في المملكة العربية السعودية من منظور قانوني**.". المجلة العربية الدولية للمعلوماتية – المجلد ٠٢، العدد ٠٣، ص٦.

2 Australian Government, office of the Australasian Information Commissioner. "What is a Privacy Policy".

القليلة القادمة، مما يزيد حجم الجدل والاهتمام الذي يصاحب هذه المواقع[١]. كما أن التطورات التكنولوجية الجديدة خلقت حالة غير مسبوقة من عمليات التعدي على الخصوصية، فمواقع التواصل الاجتماعي لا يمكن الانضمام إليها دون تقديم بيانات شخصية تقود إلى امتلاك حساب شخصي هناك، وهي البيانات التي تتحول إلى كميات هائلة من المعلومات الشخصية، يتم معالجتها للتعرف على الأنماط السلوكية، وربطها بمعدلات الربح والتسويق المختلفة[٢]. على سبيل المثال، سياسة الخصوصية في فيسبوك تسمح للطرف الثالث باستخدام البيانات التالية بهدف الدعاية وابحاث السلوك التجاري، وشركات التسويق، ومن هذه البيانات: معرفة وتحديد موقع الدخول، وقت وتاريخ تفاعلك بالموقع، المعلومات الشخصية، التوجهات والرغبات والسلوكيات الشرائية عن طريق الأطراف الثالثة ومشاركة البيانات مع الأطراف الثالثة، الاحتفاظ بالصور الشخصية والاحتفاظ بالمواقع التي تتم مشاركتها على صفحتك.[٣]

حيث إن البيانات الشخصية التي يقدمها المستخدمون توفر فرصاً ذهبية للشركات المختلفة، من أجل دراسة وفهم الأفراد عبر مستويات غير مسبوقة وهي المعلومات التي باتت أمراً ضرورياً لا يمكن التخلي عنه للبائعين عبر الإنترنت، من أجل تقديم خدمات مخصصة يؤدي عدم توفرها إلى تدهور جودة الخدمات المقدمة من خلال الشبكة العنكبوتية[٤]. وتبدو المساعي المستمرة الرامية إلى الحصول على المعلومات الخاصة لدى الأفراد نابعة من هدفين

1 Such, Jose M. & Criado, Natalia. (2021) **"Multiparty Privacy in Social Media"** Communications of the ACM, Vol. 61 No. 8, Pages 74-81

2 Weber, Rolf H. (2015). **"The digital future e A challenge for privacy?"** Computer Law & Security Review 31(2) P234-242.

٣ الزهراني، يحيى بن مفرح، **مرجع سابق**، ص ٧-٨.

4 Begie, Ghazaleh. & Liu, Huan. (2018). **"Privacy in Social Media: Identification, Mitigation and Applications"** ACM Trans. Web, Vol. 9, No. 4, Article 39.

الأول لأغراض مشروعة ترتبط بالبعد التسويقي والتجاري، أما الثاني فيرتكز على أغراض غير مشروعة تنتهي بالابتزاز وجملة أخرى من الجرائم الالكترونية. إلا أن عملية الإفصاح عن الخصوصية عبر مواقع التواصل الاجتماعي تنقسم إلى نوعين: الأول هو الكشف عن الهوية، أما الثاني فيتمثل في الكشف عن السمات، تماماً كما فعلت " Netflix نيتفليكس " خلال وقت سابق حينما قامت بنشر أفلام وفق تصنيفات محددة، مرتبطة باهتمامات ما يزيد عن (٥٠٠) ألف مشترك هناك[1].

الفرع الثاني: مخاطر الإفصاح عن الخصوصية ودرجاتها

يعيش العالم مرحلة حاسمة في ظل اعتماد مواقع التواصل الاجتماعي على سحب بيانات المستخدمين وبناء رؤيتها التسويقية عليها، مما قد يخلق صراعاً سياسياً مرتقباً، يضع الأمن القومي والازدهار الاقتصادي والرفاه الاجتماعي للدول المختلفة أمام مفترق طرق، حال عدم فرض قوانين تحد من تحكم هذه المواقع بخصوصيات الأفراد[2].

وتتعدد صور البيانات الشخصية بحسب عوامل الزمان والمكان التي تصنف بعض البيانات كبيانات شخصية توجب الحماية لها. وهي البيانات التي باتت هدفاً للعديد من المخترقين والقراصنة الالكترونيين، والساعين وراء اختراق خصوصيات مستخدمي مواقع التواصل الاجتماعي المختلفة.

ويذكر سامح التهامى ٢٠١٨ هذه الصور كالآتي: الاسم واللقب، الصوت والصورة للفرد، الأرقام الشخصية، العنوان، الحالة الاجتماعية، الخصائص الجسمانية، الحالة الصحية، الأصول العرقية، الجنسية، الآراء السياسية والمعتقدات الدينية، نتائج الاختبارات النفسية، البصمة، رقم الحساب

1 Ibid.

2 Gritzalis, Dimitris. & Others. (2014). **"History of Information: The case of Privacy and Security in Social Media"** Information Security & Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business

البنكي، عنوان البريد الالكتروني، عنوان الكمبيوتر (IP)، رقم الهاتف أو السيارة.[١] وتظهر الخطورة الحقيقية المعرضة لها هذه البيانات التي يرتكز عليها عمل مواقع التواصل الاجتماعي، قيام الأخيرة بالاستفادة من المعلومات الشخصية للمستخدمين وتسريبها في بعض الأحيان، دون موافقة المستخدمين أنفسهم، وذلك من خلال معالجة هذه البيانات واستخدامها لأغراض مختلفة، مثل التسويق، وهو انتهاك صارخ للخصوصية خاصة ذات العلاقة بالمعتقدات السياسية والدينية، مما دفع الكثيرين للمطالبة بفرض حقوق رقمية على هذه المواقع بهدف حماية المستخدمين في عالم الانترنت[٢]

وحرصت العديد من مواقع التواصل الاجتماعي على إثبات مسؤوليتها تجاه هذا الأمر، بمنح المستخدمين فرصة الإفصاح عن بياناتهم الشخصية بمحض إرادتهم أو إبقاءها سرية، على سبيل المثال، يمنح موقع انستقرام مستخدميه فرصة الإبقاء على سرية حساباتهم لمن هم خارج قائمة الأصدقاء، فيما يتيح فيس بوك للمستخدمين عرض المنشورات للأصدقاء فقط، أو تحديد قائمة من المقربين الذين يحق لهم رؤية ما يتم نشره من صور خاصة ومعلومات مختلفة[٣]. لكن الحاجة إلى بناء علاقات أو صداقات جديدة عبر مواقع التواصل الاجتماعي، يتطلب العمل على الكشف عن بعض البيانات الخاصة، لتصبح هذه الصداقات بمثابة خطوة أولى نحو تسريب الخصوصية

١ سامح، التهامي. (٢٠١٨). "نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها: دراسة في القانون الاماراتي". مجلة البحوث القانونية والاقتصادية. ص٦٢٤-٦٣٢.

2 Gritzalis, Dimitris. & Others. (2014). **"History of Information: The case of Privacy and Security in Social Media"** Information Security & Critical Infrastructure Protection Research Laboratory

Dept. of Informatics, Athens University of Economics & Business

3 Elena Zheleva & Lise Getoor,(2009) **To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles**, DBLP

والكشف عنها بإرادة المستخدمين أنفسهم.[1] ويعود ذلك إلى توجهات غالبية مواقع التواصل الاجتماعي في الاعتماد على مشاركة الفرد لبياناته ومعلوماته الخاصة كأساس في عمل هذه المواقع والمشاركة فيها، حتى أصبح مشاركة عدد كبير من المعلومات الشخصية لعدد لا منتهي من الأفراد الآخرين أمراً مقبولاً رغم خطورته. المثير للجدل أن هذا الكم الكبير من بيانات الخصوصية التي يتم تحميلها ومشاركتها عبر مواقع التواصل الاجتماعي المختلفة، تتم بإرادة المستخدمين أنفسهم، مما يضع هذه المواقع أمام الحاجة إلى مسؤوليات أكبر لحماية مستخدميهم والحفاظ على خصوصياتهم[2].

ورغم المحاولات الدولية والوطنية في إصدار قوانين وتشريعات تهدف إلى حماية خصوصية الأفراد، تماماً مثل الاتفاقية الأوروبية لحقوق الإنسان والدساتير الوطنية للدول الأعضاء في الاتحاد الأوروبي، وميثاق الحقوق الأساسية للاتحاد الأوروبي، إلى جانب تشريعات حماية البيانات، إلا أن هذه القوانين والتشريعات واجهت صعوبات كبرى في التعامل مع الواقع الذي فرضته مواقع التواصل الاجتماعي بفضائها الالكتروني، والتي رغم كونها مفيدة للمجتمع ككل فقد خلقت مشكلة معقدة في عملية حماية خصوصية الأفراد[3]. حيث إن أغلبية مستخدمي مواقع التواصل الاجتماعي هم من فئة المراهقين الذين يميل بعضهم الى عدم الاهتمام بمصطلح الخصوصية ورفضها كقيمة، بينما البعض الآخر يجهل طبيعة الانتهاك التي تقوم به هذه المواقع عبر سياساتها للخصوصية. وسنتطرق في المطلب الثاني بذكر عدد من الأمثلة لهذه الانتهاكات لحق الفرد في الخصوصية المعلوماتية.

1 Ibid

2 Jose M. Such & Natalia Criado, (2021) **Multiparty Privacy in Social Media**, Communications of the ACM, Vol. 61 No. 8, Pages 74-81

3 Rolf H. Weber (2015) **The digital future e A challenge for privacy?** Computer Law & Security Review 31(2)

المطلب الثاني: أمثلة على أشكال الانتهاكات والجرائم الالكترونية المهددة لحق الخصوصية المعلوماتية

أسفرت شبكة الإنترنت ومواقع التواصل الاجتماعي عن ظهور أشكال جديدة من الجرائم التي عرفت بالجرائم الإلكترونية، التي يقودها مختصون اشتهروا بمصطلح " قراصنة الانترنت " والتي تتضمن انتحال الشخصية، تهديد الأفراد، تشويه السمعة، التحريض على أعمال غير مشروعة، الاستيلاء على حسابات البنوك، انتهاك حقوق الملكية الفكرية والأدبية، اختراق الأنظمة، التجسس، التحرش الجنسي، التنمر الالكتروني، وهي الجرائم التي ترتكز في مجملها على معلومات مسربة من خصوصيات الأفراد. وترتكز الدوافع الإجرامية في هذا الجانب على اعتبار الكشف عن الخصوصية في مواقع التواصل الاجتماعي بمثابة انتهاك لحقوق الآخرين من الأشخاص أصحاب هذه البيانات الخاصة، وصولاً إلى التحكم بهم وابتزازهم أو تهديدهم من خلال فضحهم ونشر هذه البيانات أمام العامة[1].

لذا بات على المستخدمين ضرورة إعادة النظر في مخاطر تقديم معلومات شخصية بين أيدي كيانات الكترونية مختلفة أبرزها تلك التجارية منها، خاصة أن هذه الشركات باتت معرضة للقرصنة، إلى جانب عدم احترام الكثير منها خصوصية هذه المعلومات فيتم بيعها لجهات أخرى لأغراض أمنية وربما سياسية[2]. وبات السباق الأبرز بين مواقع التواصل الاجتماعي في الوقت الراهن، معتمداً على ارتفاع مستوى الحفاظ على الخصوصية بين أروقتها الالكترونية، فمواقع مثل " سيجنال " تفخر باعتبارها غير مملوكة لجهات كبرى

1 Elena Zheleva & Lise Getoor,(2009) **To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles**, DBLP

2 Rolf H. Weber (2015) **The digital future e A challenge for privacy?** Computer Law & Security Review 31(2)

أو دول عظمى، مما يضع معلومات الأفراد وبيانات المستخدمين بين أيدي أمينة، وأساليب مشفرة تجعل من فكرة الإطلاع عليها أمراً مستحيلاً.

حيث إن الخصوصية المعلوماتية تعد واحدة من أبرز الحقوق التي كفلتها مختلف القوانين للإنسان في كافة أنحاء العالم، بعد مساعي جادة قامت بها الدول العالمية لفرض قوانين تواجه ما تتعرض له الخصوصية المعلوماتية من خطر كبير بفعل الجرائم والانتهاكات الالكترونية المتعددة. وفي هذا المطلب سنسلط الضوء على تعريف الجرائم الالكترونية، مع لمحة تاريخية عن ظهورها، وأنواع الجرائم الالكترونية وطرق مواجهتها، ومدى الخطر الذي تشكله هذه الجرائم على الحق في الخصوصية المعلوماتية لدى الأفراد.

الفرع الأول: نشأة ومراحل تطور الجرائم الالكترونية وأنواعها

تعرف الجرائم الالكترونية باعتبارها مجموعةً من التجاوزات والأخطاء التي تؤدي إلى إحداث ضرر كبير بحق خصوصية الأفراد والشركات المستخدمة لشبكة الإنترنت بصورتها العامة ومواقع التواصل الاجتماعي على وجه الخصوص، وصولاً إلى انتهاك حقوقهم المختلفة، والهجوم على بياناتهم المحفوظة في الخزائن المحوسبة. وتصنف الانتهاكات الالكترونية كجرائم حقيقية يعاقب عليها القانون، باعتبارها أعمال إجرامية ترتكز على أجهزة الحاسوب والشبكات، وتتخذ من تقنية المعلومات مصدراً لهذه الجريمة أو أداة أو هدف أو مكان من أجل تحقيقها، بهدف الوصول غير القانوني إلى بيانات أشخاص آخرين وابتزازهم والسيطرة على أموالهم بطرق غير مشروعة.[١]

بالعودة الى تاريخ القرصنة كمثال لنشأة احدى الجرائم الالكترونية، نرى أنها ظهرت للمرة الأولى في الستينيات من القرن الماضي، في معهد ماساشويستس للتكنولوجيا، حيث كان يُنظر إلى الاختراق في ذلك الوقت باعتباره تقنية أنيقة وذكية تتيح لمستخدميها فرصة القيام بأي شيء على جهاز

١ John Baiden, Cybercrimes, 2011.

الحاسوب، مما يعني أن دور القرصنة في الماضي كان يقتصر على استكشاف كل ما هو جديد، قبل أن يتحول هذا المصطلح ليصف مجرمي الحاسوب والشبكة العنكبوتية فقط.[١] ويمكن القول إن أول جريمة كبرى في عالم القرصنة الالكترونية وقعت في العام ٢٠٠٠، واستهدفت ما يزيد عن ٤٥ مليون مستخدم للحواسيب منتشرين حول العالم، عبر فيروس خطير تم إرساله بأعداد كبيرة، أصاب الكثير من المؤسسات بالشلل التام، بعد سيطرته على الحواسيب هناك، واستحواذه على الملايين من المعلومات بصورة غير قانونية[٢].

•مراحل تطور الجرائم الالكترونية

وفقاً للتقديرات الراهنة، ينضم ما يزيد عن ٢ مليار شخص إلى الشبكة العنكبوتية لأهداف متعددة، مع وجود ٥ مليارات مستخدم للهواتف المحمولة حول العالم، وسط تبادل ما يصل إلى ٢٩٤ مليار رسالة بريد الكتروني و٥ مليارات رسالة هاتف نصية بصورة يومية، مما يجعل هذه الأرقام الكبيرة قاعدة هامة لعمل القراصنة في مجال الجرائم الالكترونية[٣]. وتشهد معدلات الجرائم الالكترونية ارتفاعاً ملحوظاً في الوقت الراهن، ففي دراسة استقصائية خلال العام ٢٠١٠، وجد الباحثون أن ٨٣% من الشركات الصغيرة وقعت ضحية بشكلٍ أو بآخر للجرائم التي تتخذ من الإنترنت منبعاً لها، بمتوسط خسائر مالية يصل بين ٢٧ ألف جنيه استرليني، حتى ٥٥ ألف جنيه استرليني[٤]. ويسعى المجرمون باستمرار إلى تطوير التقنيات المتقدمة التي تستخدم في تنفيذ جرائمهم الالكترونية المتعددة، من خلال تغيير أهدافهم، والتركيز بشكل أقل

1 Ibid

2 Kundi & Nawaz, (2014) **Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge To Governments In Developing Countries**, Issues of E-Learning in Higher Education Institutions of Pakistan

3 Ibid

4 Ibid

على سرقة المعلومات المالية، مع المضاعفة من مهام التجسس التجاري والوصول إلى المعلومات الحكومية، معتمدين بصورة كبيرة على البرامج الضارة ورسائل البريد الالكتروني العشوائية، والتسلل إلى مواقع الشركات والسيطرة على بياناتها السرية.

ويمكن القول أن الهجمات الإلكترونية باتت بديلاً عن الحرب المسلحة في طريق استنزاف الدول المعادية، ففي العام ٢٠١٠، كشفت السلطات الإيرانية عن تعرض برنامجها النووي لهجوم منظم عبر فيروس الحاسوب الشهير (Stuxnet)، والذي كان يخطط لتعطيل أجهزة الطرد المركزي الخاصة بعمليات تخصيب اليورانيوم الإيراني في ذلك الوقت[1]. ونجح العلماء في التوصل إلى نظرية علمية جديدة تحمل اسم " الجرائم الالكترونية " وهي النظرية التي برزت على يد الباحث جانشانكر، وتفترض أن الأشخاص ذوي السلوك الإجرامي المكبوت في الفضاء المادي، يميلون إلى ارتكاب الجرائم المختلفة في الفضاء الالكتروني، وهي الجرائم التي لا يملك هؤلاء الأشخاص الجرأة أو القدرة على ارتكابها في الفضاء المادي بسبب الواقع والموقف[2]. وبحسب هذه النظرية فإن قراصنة الفضاء الالكتروني، يملكون الجرأة الكافية لارتكاب جرائمهم بفعل القدرة على اخفاء هويتهم في عالم الإنترنت، لكن هذا الأمر سينعكس سلباً في المستقبل على حياتهم الواقعية، ويمنحهم الجرأة التدريجية وصولاً إلى قيامهم بارتكاب جرائم جديدة في الفضاء المادي.

•أنواع الجرائم الالكترونية

يمكن تقسيم الجرائم الإلكترونية إلى فئات، الأولى هي الجرائم التي تستهدف الشبكات وأجهزة الحاسوب بصورة مباشرة، أما الثانية فهي الجرائم التي تسهلها شبكات وأجهزة الحاسوب الآلي للوصول إلى هدفٍ مستقل عن

1 *Ibid*

2 K. Jaishankar, Establishing a Theory of Cyber Crimes, 2007.

جهاز الحاسوب وشبكة الإنترنت[١]. ويرتكز الشكل الاكثر انتشاراً في الجرائم الالكترونية على استخدام برامج قرصنة تؤدي إلى وقوع الضحايا في المحظور فور القيام باستخدامها، كل ذلك يتحقق عبر روابط مزيفة أو رسائل وهمية، تقود إلى تحفيز المستخدمين نحو استخدامها، وفور النقر عليها ينجح قراصنة الإنترنت في السيطرة على كافة البيانات والملفات المتواجدة داخل جهاز الضحية، فيصبح أسيراً لابتزازهم وطلباتهم المستقبلية[٢]. ويعد أساس هذا النوع من الجرائم هو وفرة البيانات الشخصية التي تتم مشاركتها من قبل المستخدمين ووضعها في شبكة الإنترنت من خلال مواقع التواصل الاجتماعي أو حتى البريد الالكتروني. مما يسهل على قراصنة الإنترنت ابتزاز الأفراد أو انتحال هويتهم.

وتضم الجرائم الالكترونية في طياتها مجموعة من الأنواع، من بينها سرقة وانتحال هوية الأشخاص الآخرين، والاحتيال والجرائم المالية، وبيع المواد المهربة والاستحواذ على المعلومات والملفات بصورة غير قانونية، والمواد الإباحية، وهي الجرائم التي يمكن حصرها في الآتي[٣]:

١)**الجرائم المالية:** مع تزايد الطلب على الخدمات المصرفية عبر شبكة الإنترنت، تضاعفت حدة الجرائم المالية التي تستهدف الاحتيال على

1 Kundi & Nawaz, (2014) **Digital Revolution, Cyber-Crimes And Cyber Legislation: A Challenge To Governments In Developing Countries**, Issues of E-Learning in Higher Education Institutions of Pakistan

2 Ghareb & Sedeeq (2018) **Electronic Crimes And The International Community Legislation: Comparative Analytical Study**, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 7, ISSUE 8

3 Ramdinmawii & Others (2015) **A Study on the Cyber-Crime and Cyber Criminals: A Global Problem,** International Journal of Web Technology, Volume: 03, Pages: 172-179

بطاقات الائتمان وسرقة أموال البنوك، من خلال الحصول على معلومات الضحايا البنكية، أو انتحال شخصية مسؤول حكومي أو أشخاص آخرين من المؤسسات المالية، بهدف الحصول على هذه المعلومات السرية.

٢)**المواد الإباحية:** تصنف المواقع ومقاطع الفيديو والصور الإباحية ضمن هذه الفئة، وهي الفئة التي وصفتها جامعة " كارنيجي ميلون" الأمريكية، عبر دراسة واسعة باعتبارها رعب جديد يتهدد هذا العصر، خاصة مع استغلال الأطفال جنسياً، والمساهمة في نشر الشذوذ، وصولاً إلى اسقاط الضحايا وابتزازهم جنسياً، وكل ذلك يبدأ من خلال التقرب منهم والسيطرة على معلومات شخصية عنهم تقود إلى تهديدهم.

٣)**الاتجار بالمخدرات:** يساهم تجار المخدرات بجزء كبير من الجرائم الالكترونية، عبر استغلال التقنيات الحديثة كالبريد الالكتروني في بيع منتجاتهم المحرمة، مع ترتيب مكان وطريقة سرية لإجراء التبادل الذي يعتمد في الغالب على خدمات التوصيل السريع، وهي ميزة تبدو مثالية للراغبين في شراء العقاقير المخدرة دون أن يتم كشفهم.

٤)**الإرهاب السيبراني:** ويشمل كافة أعمال الإرهاب المرتكبة في الفضاء السيبراني، وقد يكون بسيطاً عبر بث معلومات الإنترنت حول تفجيرات يُنتظر وقوعها في المستقبل، ويعرف الارهابيون السيبرانيون بأنهم أولئك الأشخاص الذين يهددون ويرغمون فرد أو منظمة أو حكومة من خلال مهاجمتهم عبر شبكة الإنترنت لتحقيق أغراض سياسية وربما شخصية.

٥)**المقامرة عبر الإنترنت:** تعد هذه المواقع واحدة من أبرز وأهم مواقع غسيل الأموال المنتشرة حول العالم، وتشكل خطوة هامة نحو الجرائم الالكترونية المعترف بها عالمياً.

٦)**التجسس والمراقبة الالكترونية:** ويقصد بها تتبع فرد أو منظمة عبر شبكة الإنترنت، وقد تشتمل على إرسال تهديدات بالقتل وغيرها، أو اسقاط

الضحية ثم ابتزازها لكسب المال غير المشروع، عبر المضايقة المستمرة في الفضاء الالكتروني.

٧)**الانتحال والخداع:** وهي واحدة من أشهر أنواع الجرائم الالكترونية، وفيها يتم انتحال شخصيات وهمية عبر البريد الالكتروني ومواقع التواصل الاجتماعي، واسقاط الضحايا لأسباب مختلفة منها مالية وجنسية.

تعد جرائم التجسس والمراقبة الالكترونية وحيازة المواد الإباحية والانتحال والخداع أنواع الجرائم التي تهدد حق الشخص في الخصوصية المعلوماتية بشكل مباشر أكثر من غيرها من الجرائم الالكترونية. حيث إن التجسس الالكتروني يعد انتهاكاً صريحاً لحرمة الفرد واحقيته في الحفاظ على بياناته الشخصية والسرية لنفسه كونها احدى مكونات مفهوم الخصوصية المعلوماتية. وتعمل الدول والحكومات العالمية على فرض خطط وقوانين وأنظمة تحارب بها هذه الجرائم الالكترونية، مع فرض عقوبات قاسية على مرتكبيها، وهو أمر تبدو الدول العربية في حاجة ماسة إلى المضي قدماً في تحقيقه، خاصة أن ضحايا الجرائم الالكترونية في الدول العربية ما زالوا في تزايد مستمر. لذا سيتطرق المبحث الثاني من هذا الفصل الثاني على بيان الجهود الدولية لمجابهة الجرائم الالكترونية المنتهكة لحق الفرد في الخصوصية.

المبحث الثاني: الجهود الدولية في حماية الحق في الخصوصية المعلوماتية

يتطرق هذا المبحث الى قياس مدى الحماية الدولية لحق الخصوصية المعلوماتية بشكل رئيسي ويتطرق لعدة عناصر أخرى كدور ومدى فعالية الاتفاقيات الدولية والمنظمات العالمية الدولية في سن القواعد القانونية الأساسية لحماية الحقوق الأساسية للإنسان. إضافة الى الضمانات القانونية التي تقدمها للفرد من خلال فرض الالتزامات القانونية على الدول. حيث إن حماية حق الفرد في الخصوصية المعلوماتية يعد تسلسلاً مباشراً من حماية حق الفرد في الخصوصية بشكل عام. إلا أن حماية أي حق من الحقوق يتطلب سلسلة من القرارات والإجراءات والخطوات السياسية والاجتماعية بشكل مستمر حتى يتشكل خط تاريخي قوي يساهم في تيسير توفير وتطبيق هذه الحماية على حق الفرد.

وبشكل أخص، تتطلب حماية الحق في الخصوصية المعلوماتية إلى خطة دقيقة وموائمة للطبيعة المتغيرة المتعلقة بهذا الحق من حيث التطور التقني المستمر. حيث يذكر لامى في دراسته "أن حماية الخصوصية في البيئة الرقمية عملية وليست إجراء، بمعنى أنها تنطلق من رؤية محددة المعالم واضحة الأهداف، وتكون مخرجاتها حزمة من الوسائل والإجراءات في ميادين التقنية والقانون وإدارة النظم التقنية بوصفها عملية تكاملية."[1] لذا يتحتم أن تحدد وتوضح الوسائل المتوفرة لحماية الحق في الخصوصية المعلوماتية، حيث إن وسائل وإجراءات الحماية هي إحدى أهم أركان الحماية لهذا الحق.

سيتطرق هذا المبحث أيضاً إلى أهمية تفعيل السلطة الدولية في فرض الالتزامات المقررة لحماية الحق في الخصوصية المعلوماتية من خلال عدة خطوات مهمة سيتم ذكرها بشكل أكثر تفصيلاً في هذا المبحث. وأهمية تعزيز المبادئ الخاصة بالقانون الدولي من حفظ لسيادة الدول، واستقلاليتها في اتخاذ

١ بارق، لامى. (٢٠١٧). "**جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني: دراسة مقارنة**". رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، ص٥٩.

القرارات، وتسوية النزاعات بطرق سلمية، وتنظيم العلاقات بين الدول. إذ أن هذه المبادئ العامة للقانون الدولي ومدى فعاليتها يؤثر بشكل مباشر في عملية ابرام الاتفاقيات الدولية المتعلقة بحماية الحق في الخصوصية المعلوماتية. حيث إن هذا الحق على وجه الخصوص، يتسم بسمات خاصة متميزة يترتب عليها عملية مختلفة وخاصة في توفير الحماية له.

حيث إنه من الجدير بالذكر أن التوجهات الدولية حول مكافحة الجرائم المعلوماتية تؤثر في مدى وجود حماية فعالة لحق الفرد في الخصوصية المعلوماتية. إلا أن هذه التوجهات تتأثر بشكل رئيسي من عدة عوامل أخرى متعلقة بمواقف الدول نحو الجرائم المعلوماتية ومدى الوعي حول تأثيرها. لإيضاح الموقف الحالي تجاه مدة الحماية المتوفرة لخصوصية الفرد المعلوماتية تجاه جرائم انتهاك الخصوصية، يفرق العبيدي، [١] ٢٠١٥ بين الاتجاهات الدولية تجاه الجرائم المعلوماتية في دراسته بعنوان "الجهود الدولية لمكافحة الجرائم المعلوماتية". الاتجاه الاول لا يرى أن للجرائم المعلوماتية طبيعة خاصة متميزة حتى يحرر لها قوانين ونصوص جديدة لمكافحتها، بل أنها حسب هذا الاتجاه جريمة كغيرها من الجرائم التقليدية وتعالج بالقوانين التقليدية الموجودة للحماية ضد أفعال مشابهة لنتائج هذه الجريمة. على سبيل المثال، تطبيق القانون العام للسرقة على جريمة معلوماتية تم فيها سرقة بيانات شخصية لفرد ما هو مثال على الاتجاه الذي يتعامل مع الجرائم المعلوماتية بنفس الوسائل المستخدمة في غيرها من الجرائم.

ينتج عن اتخاذ هذا الاتجاه التقليدي خلق عدة سلبيات منها عدم تناسب العقوبة المقررة على الجريمة بحيث إنها لا توفي وتواسي الضرر الناتج عنها، ولا تعاقب الجاني وفقاً لما ارتكبه من فعل بل بحسب ما يقرره القانون الواجب التطبيق في جريمة مشابهة. حيث إنه يتوجب من العقوبة الجنائية أن تأخذ

١ أسامة، العبيدي. (٢٠١٥). "**الجهود الدولية لمكافحة الجرائم المعلوماتية**"، مجلة الحقوق، مج ٣٩، ع ٤، ص١١٧.

بعين الاعتبار الركن المعنوي والمادي للجريمة وقياس مدى ضررها القريب والبعيد لقياس العقوبة المناسبة لها. الاتجاه الثاني من الاتجاهات الدولية تجاه الجرائم المعلوماتية ينص على انه للجرائم المعلوماتية طبيعة خاصة تميزها عن غيرها من الجرائم، مما يوجب اصدار قوانين خاصة أو تعديل القوانين الموجودة لتتعامل مع هذا النوع من الجرائم وفقاً لطبيعتها واختلافها. نتيجة لهذا الاختلاف في الاتجاه الدولي نحو الجرائم المعلوماتية، يصعب على المجتمع الدولي توفير الحماية الكافية اللازمة لحق الفرد في الخصوصية المعلوماتية من الانتهاكات التي قد تقع في دول تتبع الاتجاه الاول التقليدي. مما يشكل عقبة امام المجتمع الدولي لتحقيق التعاون الدولي. لذا سيتطرق هذا المبحث إلى نقاش الصعوبات والتحديات التي تواجه المجتمع الدولي عند مكافحة الجرائم الالكترونية بشكل عام وجرائم انتهاك الخصوصية بشكل أخص.

المطلب الأول: دور الاتفاقيات والمعاهدات الدولية في تعزيز وتأكيد مبدأ حماية الخصوصية المعلوماتية للأفراد

يتميز القانون الدولي بخصائص كثيرة ومؤثرة في المسيرة التاريخية للأحداث العالمية المتعلقة بحقوق الإنسان وكل ما يتعلق بتوفير جودة الحياة المثالية لكل فرد في العالم. إلا أن العديد من التحديات تواجه المجتمع الدولي عند مكافحة الجرائم المعلوماتية لما تختص به من سمات خاصة تميزها عن بقية الجرائم العادية. التحدي الاول والاساسي لمواجهة الجرائم المعلوماتية ومنها جرائم التعدي على الخصوصية هو اختلاف المفهوم الدولي للجرائم المعلوماتية ولمفهوم الخصوصية المعلوماتية بشكل أخص.

حيث إن هذا الاختلاف في المفهوم ينعكس على الأنظمة والقوانين التي تحرر لمكافحة هذا النوع من الجرائم مما يترتب عليه تجريم بعض اشكال الاعتداء على الخصوصية في نظام معين وعدم تجريم البعض الآخر في نظام آخر. إلا أن هذا الاختلاف التشريعي قد يتعرض للاستغلال من قبل المجرمين عند ارتكابهم الاعتداء تحت نظام تشريعي لا يردع هذا الفعل. نظراً لسهولة التلاعب في الأدلة الرقمية التي تسمح للجاني بتغيير موقع ارتكابه الجريمة

أو الأداة المستخدمة خلالها. ويعدد العبيدي ٢٠١٥، الصعوبات التي تواجه المجتمع الدولي كالآتي: عدم الاتفاق على مفهوم موحد للجرائم المعلوماتية، عدم وجود تعاون فيما يتعلق بالإجراءات الجنائية، اختلاف النظم القانونية الإجرائية، مشكلة تنازع الاختصاص القضائي، عدم وجود قنوات للاتصال بين الدول، التوافق في تجريم ذات الفعل في كل من التشريع الوطني والدولي، واخيراً عدم وجود معاهدات ثنائية او جماعية بين الدول.[١] لذا يكمن الدور الرئيسي للاتفاقيات الدولية في المساهمة في تحقيق التعاون بين الدول في مكافحة الجرائم التي يتعدى نطاقها الحدود الجغرافية للدول كجرائم التعدي على الخصوصية المعلوماتية.

•دور منظمة الأمم المتحدة في حماية الحق في الخصوصية المعلوماتية

وبالعودة إلى دور الاتفاقيات والمعاهدات الدولية في حماية خصوصية البيانات، نستعرض أهم المساهمات الدولية في الاعتراف وتعزيز هذا الحق من قبل ثلاثة من أكثر المنظمات الدولية فعاليةً ونشاطاً في المجتمع الدولي. الاولى وهي منظمة الامم المتحدة لحقوق الإنسان والتي ساهمت بعدة أدوات منها الإعلان العالمي لحقوق الانسان الذي أعلنته الجمعية العامة للأمم المتحدة في عام ١٩٤٨م والذي تضمن في المادة ١٢ الإشارة الى أهمية الحق في الخصوصية كإحدى الحقوق الانسانية المهمة والمرتبطة بشكل رئيسي بكرامة الانسان وكيانه. على الرغم من أن هذه المادة لا تمتلك خاصية الالزام القانوني إلا أن مبادئها أثرت في كثير من المعاهدات الدولية والصكوك الإقليمية لحقوق الإنسان والدساتير الوطنية. وفي عام ١٩٦٦م أكثر من ١٦٠ دولة دخلت كطرف في الاتفاقية الدولية للحقوق المدنية والسياسية، والتي تضمنت في المادة ١٧ على التالي " (١) لا يجوز تعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصيته أو أسرته أو منزله أو المراسلات، ولا

١ المرجع السابق، ص ١١٩-١٢١.

الاعتداء غير المشروع على شرفه وسمعته. (٢) لكل فرد الحق في حماية القانون من مثل هذا التدخل أو الهجمات."[١]. وتتميز هذه المادة بإلزاميتها القانونية على الدول الأطراف في هذه المعاهدة بعكس ما طرحه الإعلان العالمي لحقوق الانسان. حيث إن الانضمام كطرف في معاهدة يلزم الدولة باحترام وتنفيذ بنود هذه الاتفاقية وفقاً للمادة ٢٦ من اتفاقية فيينا لقانون المعاهدات[٢] والذي ينص على ان كل معاهدة نافذة ملزمة لأطرافها وعليهم تنفيذها بحسن نية وهذا ما يميز الاتفاقيات الدولية غيرها من الادوات الدولية في حل النزاعات ومكافحة الجرائم المعلوماتية.

•دور مجلس أوروبا في حماية الحق في الخصوصية المعلوماتية

ومن جانب آخر، يساهم مجلس أوروبا كمنظمة دولية يهدف إلى حماية حقوق الإنسان وتعزيز مبدأ الديموقراطية وسيادة القانون. ومن مساهماتها في تعزيز الحق في الخصوصية المعلوماتية هي اتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية ١٩٨١، وتعد هذه الاتفاقية أول صك دولي ملزم قانونيًا بشأن حماية البيانات وأتيحت للتوقيع حتى من قبل الدول غير الأعضاء في مجلس أوروبا.[٣] وتقدم هذه الاتفاقية الحماية للأفراد من التعديات المصاحبة لجمع ومعالجة البيانات الشخصية والتي تسعى إلى تنظيم التدفق عبر الحدود للبيانات الشخصية في نفس الوقت. وتوفير الضمانات فيما يتعلق بجمع البيانات الشخصية "الحساسة" وذلك من خلال حظر معالجة

1 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966. Article 17.

2 Vienna Convention on the Law of Treaties, Done at Vienna on 23 May 1969. Entered into force on 27 January 1980. United Nations, Treaty Series, vol. 1155, p. 331.

3 Treaties and International Agreements on Privacy & Data Protection. International and Foreign Cyberspace Law Research Guide. Georgetown law library

البيانات المتعلقة بالعرق، والتوجه السياسي، والمعلومات الصحية، والدين، والسجل الجنائي، والحياة الجنسية، وما إلى ذلك. وتضمن هذه الاتفاقية أيضا في حال غياب الضمانات القانونية المناسبة حق الفرد في معرفة المعلومات المخزنة عنه او عنها، وإن لزم الأمر في تصحيحها. وفي سنة ٢٠٠١، طرح بروتوكول إضافي فيما يتعلق بالسلطات الرقابية وتدفقات البيانات عبر الحدود، إلى اتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية. وتتضمن هذه الإضافة على إنشاء سلطات وطنية لحماية البيانات وذلك من خلال رصد مستوى الامتثال للقوانين المعتمدة وفقًا للاتفاقية الأصلية وتنظيم عمليات نقل البيانات عبر الحدود الوطنية.

وفي عام ٢٠١٨، أصدر مجلس أوروبا بروتوكول تعديل لاتفاقية حماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية (لم يدخل البروتوكول حيز التنفيذ بعد)، والذي يهدف الى تحديث وتحسين الاتفاقية الاصلية لعام ١٩٨١م وذلك من خلال مراعاة التحديات التي تطرحها الأشكال الجديدة لتكنولوجيا المعلومات والاتصالات. ويعد هذا التعديل من أكثر البروتوكولات التقدمية في مجال حماية الحق في الخصوصية المعلوماتية وهذا لما شملته من متطلبات أقوى فيما يتعلق بمبادئ التناسب وتقليل البيانات، وقانونية معالجة البيانات، توسيع مصطلح البيانات "الحساسة" ليشمل البيانات الجينية والبيو مترية، والعضوية النقابية والأصل العرقي. فرض الالتزام بالإعلان عن انتهاكات البيانات، وزيادة الشفافية في معالجة البيانات، وإضافة حقوق جديدة للأشخاص في مجال اتخاذ القرارات الخوارزمية، والتي لها صلة خاصة بتطوير الذكاء الاصطناعي؛ تعزيز مسؤولية مراقبي البيانات، اشتراط الالتزام بمبدأ "الخصوصية حسب التصميم" والذي ينص على أهمية الالتزام بإعطاء الأولوية لخصوصية الأفراد عند تصميم وخلق تقنيات وأنظمة جديدة. "الخصوصية حسب التصميم هي نهج يتم اتباعه عند إنشاء تقنيات وأنظمة جديدة. يحدث ذلك عندما يتم دمج الخصوصية في التكنولوجيا والأنظمة بشكل تلقائي. هذا يعني أن منتجك مصمم مع مراعاة الخصوصية كأولوية، إلى جانب

أي أغراض أخرى يخدمها النظام."[1]. ونص هذا التعديل أيضاً على تطبيق مبادئ حماية البيانات على جميع أنشطة المعالجة، بما في ذلك ما يتعلق بالأمن القومي، مع استثناءات وقيود محتملة تخضع للشروط التي تحددها الاتفاقية، ونظام واضح لتدفقات البيانات عبر الحدود، وأخيراً تعزيز الصلاحيات والاستقلالية لسلطات حماية البيانات وتعزيز الأساس القانوني للتعاون الدولي.

•السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان فيما يخص انتهاكات الخصوصية

المحكمة الاوروبية لحقوق الإنسان هي مؤسسة قانونية متخصصة أسست عام ١٩٥٩م مرتكزة على الاتفاقية الاوروبية لحقوق الإنسان (ECHR)، وهي مسؤولية عن ضمان امتثال الدول الأطراف في الاتفاقية الأوروبية لحقوق الإنسان لالتزاماتها بموجب الاتفاقية[2]، بما في ذلك المادة ٨ والتي تنص على "إن لكل فرد الحق في احترام حياته الخاصة والعائلية ومنزله ومراسلاته. ولا يجوز لأي سلطة عامة أن تتدخل في ممارسة هذا الحق إلا إذا كان ذلك وفقاً للقانون ويكون ضرورياً في مجتمع ديمقراطي لصالح الأمن القومي أو السلامة العامة أو الرفاه الاقتصادي للبلاد، للوقاية من الفوضى أو الجريمة أو لحماية الصحة أو الآداب العامة أو لحماية حقوق الآخرين وحرياتهم.، التي تعترف بالحق في الخصوصية."[3] إضافة إلى الشكاوى المتعلقة بانتهاكات حقوق الإنسان المقدمة من الأفراد أو مجموعات الأفراد ضد دولة عضو وكذلك الشكاوى المقدمة من دولة عضو ضد دولة عضو أخرى.

1 7 Principles of Privacy by Design, Internet Privacy Guy. Nov 20, 2017.

2 European Court of Human Rights, Europe's Human Rights Watchdog.

3 Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.

وبدورها المحكمة الأوروبية لحقوق الإنسان تشارك بيانات الحقائق والتي تشمل ملخصات الأحكام الصادرة عن المحكمة الأوروبية لحقوق الإنسان في عشرات القضايا المتعلقة بحماية البيانات والحق في الخصوصية. ومنها بيان وقائع المحكمة الأوروبية لحقوق الإنسان بشأن حماية البيانات الشخصية، وبيان وقائع المحكمة الأوروبية لحقوق الإنسان بشأن التقنيات الجديدة.

ومن هذه القضايا قضية "كات" والمملكة المتحدة[1]، حيث تتعلق هذه القضية بشكوى مقدمة من قبل ناشط يدعى كات والذي يناهز عمر الـ٩٤ سنة، وهو متظاهر سلمي كان يحضر المظاهرات العامة بانتظام منذ عام ١٩٤٧م. وفي عام ٢٠٠٥م، بدأ في حضور المظاهرات التي نظمتها "سماش إيدو". على الرغم من أنه كان هناك في كثير من الأحيان اضطراب وإجرام خطير في احتجاجات "سماش ايدو"، إلا أن السيد كات لم يحضر إلا بشكل سلمي ولم يتم اتهامه بأي شيء. وتتضمن شكواه على اعتراضه على جمع بياناته الشخصية والاحتفاظ بها في قاعدة بيانات الشرطة تحت قاعدة البيانات بمسمى "المتطرفين المحليين". ورأت المحكمة أنه تم انتهاك المادة ٨ من الاتفاقية وذلك لأن البيانات المحفوظة عن "كات" تتعلق بآرائه السياسية وهي من البيانات الشخصية التي تتطلب حماية خاصة وفقاً للاتفاقية الاوروبية لحقوق الإنسان. وأضافت المحكمة ان مقدم الشكوى ليس لديه تاريخ اجرامي او احتمالية ارتكابه لجريمة، وختمت المحكمة موقفها حول ذلك بأن جمع المعلومات عن مقدم الشكوى يعد تصرفاً مبرر، الا أن الاحتفاظ بها رغم اقتصار ضمانات السلامة لها يعد تصرفاً غير مبرر.

1 The Catt that got the cream – retention of data concerning peaceful protestor was an unlawful interference with article 8, UK Police Law Blog. Serjeants'Inn Chambers.

في هذه القضية ادعى المدعى "ايكاغير" ضد فرنسا[1] انتهاك حقه في احترام حياته الخاصة حين أدين إدانة جنائية نتيجة رفضه لطلب تقديم عينة بيولوجية منه ليتم انضمامه لقاعدة البيانات المحوسبة الوطنية للحمض النووي. ورأت المحكمة أنه تم انتهاك المادة ٨ من الإتفاقية الأوروبية لحقوق الانسان في هذه القضية، ونوهت المحكمة أيضا إلى أنه لم يتم اتخاذ أي إجراء مناسب حتى الآن بشأن تحديد مدة حفظ البيانات الشخصية للأفراد بناءً على الغرض من الملف المخزن وطبيعة و / أو خطورة الجرائم المعنية في هذه الحالة. كما أن المحكمة في هذه القضية قضت بأن السياسات الخاصة بحفظ الحمض النووي في قاعدة البيانات المحوسبة الوطنية للحمض النووي لم توفر الحماية الكافية لأصحاب البيانات بسبب عدم تحديد مدة حفظ هذه البيانات وعدم إمكانية حذفها بعد تخزينها. ويعد هذا مثالاً على فشل هذه الجهة في الموازنة بين المصالح التنافسية العامة والخاصة.

ومن القضايا أيضاً ما لم يخالف الإتفاقية الأوروبية لحقوق الإنسان إلا أنها توضح جوانب مهمة من الخصوصية المعلوماتية والحدود التي يضعها القانون للسلطات التقديرية. كقضية برايز ضد ألمانيا [2]، ووقائعها تقوم على الشكل الاتي: وفقًا لتعديلات عام ٢٠٠٤ على قانون الإتصالات الألماني، ألزمت الشركات بجمع وتخزين البيانات الشخصية لجميع عملائها، بما في ذلك مستخدمو بطاقات SIM مسبقة الدفع، والتي لم تكن مطلوبة من قبل. المدعيين هم من نشطاء الحريات المدنية ومنتقدو نظام مراقبة الدولة، كانوا مستخدمين لهذه البطاقات لذلك كان لا بد من تسجيل بياناتهم الشخصية، مثل أرقام هواتفهم وتواريخ الميلاد والاسم والعنون مع مزودي الخدمة. وكان مضمون شكواهم هو تخزين بياناتهم الشخصية عند شرائهم بطائق الـ SIM

1 Collection of Personal Data Cases, European Court of Human Rights.p17.

2 Collection of Personal Data Cases, European Court of Human Rights.p20.

مسبقة الدفع. وعلى ذلك قررت المحكمة أنه لم يتم انتهاك المادة ٨ من الاتفاقية الاوروبية لحقوق الانسان، نظراً بأن المانيا لم تتجاوز حدود سلطتها التقديرية في تطبيق القانون المعني، وعند اختيار وسائل تحقيق الأهداف المشروعة لحماية الأمن القومي ومكافحة الجريمة، وأن تخزين البيانات الشخصية لمقدمي الدعوى كان متناسبًا و "ضروريًا في مجتمع ديموقراطي ". وبالتالي لم يكن هناك انتهاك للاتفاقية. واعتبرت المحكمة بشكل خاص أن جمع أسماء المدعيين وعناوينهم كمستخدمين لـ شرائح سيم لم يتجاوز حد التدخل المسموح في حقوقهم وأضافت المحكمة إلى أن القانون المعني في هذه القضية احتوى على ضمانات إضافية من خلال إمكانية الأشخاص باللجوء إلى هيئات مستقلة للإشراف على البيانات ليقوموا بمراجعة طلبات البيانات من السلطات والسعي إلى تقديم التصحيح القانوني إذا لزم الأمر.

وفي ليندر ضد السويد[1]، تعلقت هذه القضية باستخدام ملف سري للشرطة في توظيف نجار، المدعي الذي كان يعمل كبديل مؤقت في المتحف البحري في كارلسكرونا، بجوار منطقة أمنية عسكرية مقيدة، اشتكى من تخزين البيانات المتعلقة بأنشطته النقابية قبل وقت طويل وإدعى أن ذلك قد أدى إلى استبعاده من الوظيفة المعنية، وزعم أنه لا يوجد شيء في خلفيته الشخصية أو السياسية ما يلزم تسجيله في سجل دائرة الأمن وتصنيفه على أنه "خطر أمني". ورأت المحكمة أنه لم يكن هناك انتهاك للمادة ٨ من الاتفاقية، وعلى الرغم من أن كلاً من التخزين في سجل سري والإفراج عن المعلومات المتعلقة بالحياة الخاصة للفرد يقعان في نطاق المادة ٨ من الاتفاقية، إلا أن المحكمة أشارت إلى أنه في المجتمعات الديموقراطية، يسمح قانونياً بوجود أجهزة الاستخبارات وتخزين البيانات وأن يكون لها الغلبة على مصلحة المواطنين

1 Ibid

بشرط أن يكون يسعى لتحقيق أهداف مشروعة، كمنع الفوضى أو الجريمة أو حماية الأمن القومي. في هذه القضية، وجدت المحكمة أن الضمانات الواردة في نظام مراقبة الأفراد السويدي تفي بمتطلبات المادة ٨ من الاتفاقية وأن الحكومة السويدية كان لها الحق في اعتبار أن مصالح الأمن القومي لها الغلبة على المصالح الفردية للمدعي.

نستنتج من هذه القضايا أن الاتفاقية الأوروبية لحقوق الإنسان تحث على حماية الآراء السياسية للأفراد وعدم انتهاكها من خلال وضع تصنيفات تمييزية للأفراد في السجلات الأمنية العامة. إضافةً الى أهمية تحديد مدة حفظ الجهات المختصة لبيانات الفرد الشخصية وتدوين الغرض من حفظها. وأضافت القضايا المذكورة أعلاه والتي لم يخالف محط دعواها الاتفاقية، بيان السماح للجهات المختصة بحفظ بيانات الأفراد المتعلقة بالخدمات التي تقدمها هذه الجهة، كشركات الاتصال وغيرها، مع مراعاة عدم تعدي الحدود التي توضحها الاتفاقية. وفي القضية الأخيرة نستنتج أن للسلطات العليا الحق في تغليب المصلحة العامة على مصلحة الفرد في القضايا الأمنية والحساسة، ويشمل ذلك أحقيتها في تخزين وحفظ البيانات الشخصية للأفراد المعنيين.

المطلب الثاني: الموقف الدولي المعاصر حول أهمية حفظ الحق في الخصوصية المعلوماتية

يتمثل الموقف الدولي المعاصر تجاه الخصوصية المعلوماتية في العمل تجاه تحقيق التوازن بين ما تقدمه أنظمة المعلومات من خدمات تعاون الدول على تحقيق الأمن الوطني كالمراقبة وجمع كم كبير من البيانات وبين حماية خصوصية الأفراد المعلوماتية من الانتهاك. وفي سبيل تحقيق هذا التوازن، ظهرت عديد من التوجهات الدولية بهذا الخصوص ومنها: قرار الجمعية العامة للأمم المتحدة رقم (٦٨\١٦٧) للعام ٢٠١٣ بشأن الحق في الخصوصية في العصر الرقمي، والذي أصدر من قبل الجمعية العامة للأمم المتحدة نتيجة الشعور بالقلق تجاه السلطة التي تملكتها الجهات الحكومية في سهولة الوصول إلى خصوصية الأفراد ومراقبتهم وتخزين معلوماتهم سواءً داخل البلد او خارجه.[١]. ويقوم هذا القرار على تعزيز حماية الحق في الخصوصية المعلوماتية من ناحيتين، إحداهما هو التأكيد على ضمان حق الأفراد في الخصوصية المعلوماتية كما جاءت به الاتفاقيات والأحكام الدولية، والثانية هي ضرورة وضع إطار عام لبقية الدول حول ما يعد انتهاكا تعسفيا لحق الخصوصية المعلوماتية.[٢] وثاني إحدى التوجهات الدولية كانت متمثلة في تقرير الحق في الخصوصية في العصر الرقمي للعام ٢٠١٤، والذي أصدر من قبل المفوض السامي في مجلس حقوق الإنسان التابع للأمم المتحدة. وكان يهدف إلى خلق إطار قانوني فعال يعزز من أهمية هذا الحق في ظل التطورات التقنية المستمرة. وتضمن هذا التقرير الى استقراء ممارسات الدول والمنظمات الدولية والمؤسسات الوطنية حول احترام الحق في الخصوصية

١ رزق، سلمودي وآخرون (٢٠١٧م). **الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي**. مجلة الجامعة العربية الأمريكية للبحوث، مجلد ٣، العدد ٢، ص١٢.

٢ المرجع السابق، ص١٣.

والتعامل معه، وخلق الموازنة بين هذه الممارسات والموقف التقليدي للقانون الدولي حول الحق في الخصوصية. ثالث التوجهات الدولية يتمثل في تقرير البرلمان الاوروبي بشأن نظام الاتصالات والذي يساهم في التعبير عن موقف الاتحاد الأوروبي من أمن المعلومات، وأخذ هذا التقرير بعين الاعتبار الاتفاقية الاوروبية لحقوق الإنسان لعام ١٩٥٠م. وعلى الرغم من أن هذه الاتفاقية في مادتها الأخيرة تشير إلى أهمية احترام الحق في الخصوصية إلا في مصلحة الأمن القومي، إلا حتى أن التدخل في هذه الحالة يجب أن يكون متناسباً وبغرض تحقيق الأمن القومي لا أقل من ذلك كرغبة او إفادةً، حيث إن مبدأ التناسب يقوم على إيجاد التوازن بين حقيقة المخاطر على أرض الواقع والمخاطر التي تبرر الغاية من المراقبة.[١]

الفرع الأول: دور المنظمات الدولية في تحقيق التعاون الدولي

تعد المنظمات الدولية إحدى أهم أركان القانون الدولي العام في تحفيز ودعم إرادة الدول نحو الوفاء بالمعايير الدولية وتشريع القوانين الدولية وغيرها من المهام الرئيسية في مكافحة الجرائم الدولية ومنها جرائم التعدي على بيانات الشخصية للأفراد. يتناول جاسم ٢٠١٩ بعض من المنظمات الدولية التي ساهمت بدورها في مكافحة الجرائم المعلوماتية بشكل أكثر كفاءة وتعاون، ومنها المنظمة الدولية للشرطة الجنائية (الانتربول) التي أنشأت عام ١٩٢٣م وتعد أكبر منظمة شرطية دولية، تهدف إلى المساهمة في تحقيق درجة عالية من التعاون الدولي في مكافحة الجرائم المعلوماتية. حيث إن أهم اهداف هذه المنظمة تتمثل في ١) جمع المعلومات المتعلقة بالجرائم والمجرمين عن طريق مراكز الشرطة الرئيسية للدول الأعضاء. ٢) ضبط الهاربين والمطلوبين من قبل الدول الأعضاء بغض النظر عن جنسياتهم، وذلك بهدف زيادة التعاون بين الدول الأعضاء. ٣) تقديم الخدمات لدعم جهود الشرطة في مكافحة

١ المرجع السابق، ص١٦.

الجرائم العابرة للحدود وذلك من خلال تقديم البيانات التالية: الأدلة الجنائية، بصمات الأصابع، والحمض النووي. ٤) المساهمة في بناء تعاون متبادل بين سلطات الشرطة الجنائية وفقاً للقوانين الوطنية للدول الأعضاء والإعلان العالمي لحقوق الإنسان.[١]

ومن المنظمات الفعالة في المساهمة في مكافحة الجرائم المعلوماتية خاصة التي تنتهك الحق في الخصوصية، هي منظمة التعاون الاقتصادي والتنمية لعام ١٩٦١م. ابتداءً من سنة ١٩٧٨م قامت هذه المنظمة بوضع قواعد ارشادية حول حماية الخصوصية ونقل البيانات الخاصة والمعالجة الالكترونية للبيانات. وتعرف المنظمة البيانات بأنها "معطيات تتوفر لها الحماية في كل مرحلة من مراحل الجمع والتخزين والمعالجة والنشر"[٢]. رغم عدم الزامية هذه القواعد إلا أنها توجيهات وتوصيات مباشرة للدول الأعضاء وغيرها من الدول. حيث إن تحرير قواعد تحمي الحق في الخصوصية بغض النظر عن الزاميتها يساهم في نشر الوعي بين الدول وتنبيههم وتذكيرهم بجوانب متعلقة بحماية هذا الحق قد تخفى عنهم. وتتضمن هذه الارشادات والقواعد ثمانية مبادئ أساسية وهي ١) تحديد حصر عمليات جمع البيانات ٢) الاقتصار على طبيعة البيانات الشخصية وتحديدها ٣) تحديد الغرض ٤) حصر الاستخدام بالغرض المحدد ٥) توفير وسائل حماية وأمن المعلومات ٦) العلانية ٧) الحق في المشاركة والمسائلة.[٣]

وعلى الصعيد الإقليمي، اعتنى الاتحاد الاوروبي بحماية الخصوصية المعلوماتية منذ منتصف السبعينات وذلك من خلال المساهمة في توحيد

١ فادية، جاسم. (٢٠١٩). "**التعاون الدولي للحد من الجرائم المعلوماتية**". مجلة كلية الحقوق – جامعة النهرين. ص٣٨٧.

٢ شريف، خاطر. (٢٠١٥). "**حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا**". مجلة البحوث القانونية والاقتصادية. العدد ٥٧، ص١٦.

٣ المرجع السابق، ص١٧.

القواعد القانونية المقررة لحماية الحق في الخصوصية، وإصدار الاتفاقيات والأدلة والتوصيات للدول. ومن هذه المساهمات "اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات الشخصية" لعام ١٩٨١م، موقعة ومصدقه من قبل ٣٩ دولة. "وعلى خلاف توصيات منظمة التعاون الاقتصادي والتنمية، فإن هذه الاتفاقية ملزمة للأعضاء الموقعين عليها- وينحصر نطاقها بالأشخاص الطبيعيين والملفات المعالجة اليا، وتطبق على الملفات المعالجة اليا في القطاعين العام والخاص"[١] وتحتوي هذه الاتفاقية على ٢٧ مادة بهدف تحقيق أهداف عدة كتحقيق الوحدة والتعاون بين الدول الأعضاء بناء على مبدأ احترام سيادة القانون وحقوق الإنسان وخصوصا الحق في الخصوصية المعلوماتية نتيجة خضوع هذا العدد الهائل من البيانات الشخصية للمعالجة الرقمية. وتشمل هذه الاتفاقية على ثمان مبادئ والتي تمثل الحد الأدنى للمعايير التي يتوجب على الدول الالتزام بها في حماية الحق في الخصوصية المعلوماتية من خلال تضمينها في التشريعات الداخلية. وهي تحقيق العدل الاجتماعي، الوقاية، قيود الجمع، العلنية، تؤقيت الغرض وتحديد المدى، مشاركة الأفراد والدقة.[٢]

نظراً لطبيعة الجرائم المعلوماتية العابرة للحدود، أصبح من السهل على المجرم أن يحضر لجريمة في بلد ما وينفذها في بلد اخر ويهرب منها لبلد ثالث. لذا أصبح التعاون الدولي ذو ضرورة قصوى ومن شتى النواحي، التشريعية والقضائية والأمنية. "فإن التعاون الدولي له النصيب في حل الإشكاليات التي تقع بين الدول، الذي يعد مبدأ التعاون الدولي في الوقت الحاضر من أهم المبادئ القانونية الدولية، الذي ظهر أهميته في مجال مكافحة الجرائم المعلوماتية مع تعدد وتشعب التطورات التي رافقت الجريمة

١ المرجع السابق، ص١٨.

٢ المرجع السابق.

وأساليب ارتكابها"[١]. ويصعب حصر مفهوم التعاون الدولي لتعريف واحد نتيجة تعدد الاشكال التي يأخذها واستمرارية تطور الأساليب والوسائل الدولية في تحقيق التعاون، إضافة إلى أن مفهوم التعاون الدولي مرتبط بشكل كبير بمفهوم الجرائم ومكافحتها بناءً على مفهومها وفقا لتشريع كل دولة. ويهدف التعاون الدولي الى تحقيق درجة عالية من التوافق والانسجام في المجتمع الدولي لتسهيل تحقيق أهدافه، وحماية القيم والمصالح الاجتماعية الدولية المشتركة.

ويعد التعاون الدولي من المبادئ الأساسية في القانون الدولي لعدة أسباب ومنها طبيعة العلاقة بين الدول مهما بلغت قوتها واستقلالها إلا أن الدول لا تستطيع أن تستغني بشكل كامل عن احتياجها للدول الأخرى بشكل أو بآخر، خاصة أن طبيعة الجرائم الحديثة أصبحت تتطلب تعاوناً بين الدول في مكافحتها. ثانيا، تعد الجرائم المعلوماتية إحدى تحديات العصر الحديث، ولذلك فإن التعاون الدولي يوفر للدول إمكانية خلق جهاز تشريعي منفصل عن القانون الوطني ليكمل أي نقص تشريعي وارد ويسمح بتحقيق التعاون المطلوب في هذه القضايا. ثالثاً، يساهم التعاون الدولي في مكافحة الجرائم بشكل عام في توحيد الكثير من القوانين المقررة لمكافحة الجرائم المعلوماتية على سبيل المثال، مما يجعل من فكرة تدويل القانون الجنائي فكرة أقرب للواقع. رابعا واخيراً، يخلق التعاون الدولي في مكافحة الجرائم رادعا إضافيا للمجرم الذي يباشر جريمته معتقداً أن الهروب لدولة أخرى قد ينجيه من العقاب، بينما يتيح التعاون الدولي في هذه الحالة للدولة التي هرب اليها أن تقبض عليه وترحله.

١ فادية، جاسم. (٢٠١٩). "**التعاون الدولي للحد من الجرائم المعلوماتية**". مجلة كلية الحقوق – جامعة النهرين، ص٣٧٩.

•أشكال التعاون الدولي

يحظى التعاون الدولي بأشكالٍ مختلفة أهمها: التعاون الشرطي الدولي، التعاون القضائي الدولي، والتعاون الدولي في مجال تسليم المجرمين، والتعاون الدولي في مجال التدريب على مواجهة الجرائم المعلوماتية. التعاون الشرطي الدولي يتضمن التعاون الدولي بين أجهزة الشرطة بين الدول المختلفة من خلال جمع المعلومات المتعلقة بالمجرمين وتعميمها بين الدول حيث إن إجراءات الشرطة العامة لا تسمح بتعقب المجرمين ومتابعتهم في حين تجاوزوا حدود الدولة. ومن الاجراءات التي تقف عقبة في تحقيق التعاون الدولي في مكافحة الجرائم المعلوماتية هي الاختصاص القضائي، على سبيل المثال، مجرم من جنسية مختلفة عن دولة ما يرتكب جريمة من حاسب الي موجود في دولة أخرى واثار الجريمة تقع في دولة ثالثة. وقد تم أخذ خطوة نحو ذلك عبر المنظمة الدولية للشرطة الجنائية (الانتربول).[١]

ويمكن القول أن التعاون القضائي الدولي يتطلب السماح بالدول الغير مختصة بالقيام بالإجراءات القضائية التي تساعدها في تحقيق هذا التعاون كملاحقة المجرم ومحاكمته وتوقيع العقوبة عليه، معاينة الأدلة كمواقع الانترنت والاقراص الصلبة وسماع الشهود والقبض على المتهمين. اما التعاون الدولي في مجال تسليم المجرمين فيشمل ابرام الاتفاقيات بين الدول التي توفر الصلاحيات للدول بتسليم المجرمين المطالب محاكمتهم. واخيراً، التعاون الدولي في تدريب وتحسين مكافحة الجرائم المعلوماتية، ويتحقق هذا التعاون بعدة خطوات أهمها: تشجيع جهات العدل على مواكبة التطورات التقنية السريعة لمعرفة مجابهتها، أخذ الاجراءات التي تساهم في توسيع نطاق تطبيق القوانين التقليدية ليوافي خصائص الجرائم المعلوماتية الخاصة.[٢]

١أسامة، العبيدي. (٢٠١٥). "**الجهود الدولية لمكافحة الجرائم المعلوماتية**"، مجلة الحقوق، مج ٣٩، ع ٤، ص١٢٢.

٢ المرجع السابق. ص١٣٤.

الفرع الثاني: الموقف القانوني الدولي حول أهمية حفظ الحق في الخصوصية المعلوماتية

عند المقارنة بين الايجابيات والسلبيات للحماية الدولية لحق الخصوصية المعلوماتية، نجد أن الفارق النسبي بينهما في تغير مستمر. تتمثل الايجابيات في أن عدد المنظمات والاتفاقيات الدولية المتعلقة بحماية الخصوصية المعلوماتية في ازدياد، التطور القضائي الدولي الايجابي حول الصعوبات التي تفرضها طبيعة جرائم الخصوصية المعلوماتية، تطور واستيعاب عدة دول لمفهوم الخصوصية المعلوماتية وأهمية حمايتها كحق أساسي، استيعاب الاخطار التي تفرضها وسائل التقنية الحديثة على الحقوق الأساسية للفرد ومنها الخصوصية، اتساع إطار الاتفاقيات حول معظم ما يخص الخصوصية المعلوماتية. على سبيل المثال، الإعلان الخاص باستخدام التقدم العلمي والتكنولوجي لمصلحة السلم وخير البشرية الصادر من الأمم المتحدة عام ١٩٧٥م بهدف منع الهيئات التابعة للدول أن تستخدم التطورات العلمية بصورة تتنافى مع ما أكده الإعلان. حيث نصت المادة السادسة منه بـ "على جميع الدول أن تتخذ تدابير تهدف إلى تمكين جميع قطاعات السكان من الإفادة من حسنات العلم والتكنولوجيا، والى حماية القطاعات، اجتماعياً ومادياً، من الآثار الضارة التي يمكن أن تترتب على سوء استخدام التطورات العلمية والتكنولوجية، بما في ذلك إساءة استعمالها على نحو يمس بحقوق الفرد أو الجماعة، خاصة فيما يتعلق باحترام الحياة الخاصة وحماية شخصية الإنسان وسلامته البدنية والذهنية."[١] وتتمثل السلبيات التي قد تواجه المجتمع الدولي عند محاولة توفير الحماية لحق الخصوصية المعلوماتية في استمرارية تطور وتغير خصائص وسائل التقنية للتواصل الاجتماعي مما يصعب مواكبتها، بطء بعض الدول في مواكبة التغيرات الدولية على الصعيد القانوني فيما يخص جرائم الخصوصية

١ جديد، صبرينة. (٢٠١٨) "**الحماية القانونية للحق في الخصوصية المعلوماتية**". مجلة التواصل في العلوم الانسانية والاجتماعية. المجلد ٢٤، العدد ٢، ص١٣١.

المعلوماتية، وقد يعود ذلك الى عدم اعتراف تلك الدول بهذا الحق كحق رئيسي يستوجب الحماية القانونية. وأخيراً، رغم تعدد الاتفاقيات والمعاهدات الدولية التي تدعم حق الفرد في الخصوصية المعلوماتية، إلا أن العديد منها يفتقر عنصر الإلزامية القانونية.

ولخلق الموازنة بين هذه الايجابيات والسلبيات، قدم المفوض السامي في مجلس حقوق الإنسان تقريراً يؤكد على عاملين مهمين في تكوين الحماية للخصوصية المعلوماتية وهما: أن يتم استقراء ممارسات الدول حول حماية ومعاملة هذا الحق لمساعدة تكوين العرف الدولي فيما يتعلق بذلك، والعامل الثاني هو خلق الموازنة بين هذه الممارسات وبين الموقف التقليدي للقانون الدولي نحو حماية الخصوصية المعلوماتية.[1] الا أن الاعتماد الغالب على ممارسات الدول كمصدر أساسي للعرف الدولي ولتكوين الموقف الدولي يؤدي الى تباطء عجلة التقدم نحو خلق إطار عصري ومواكب لمتغيرات الخصوصية المعلوماتية.

١ زينب، الضناوي. (٢٠١٩). "**الحماية القانونية للخصوصية على الانترنت في ظل الجهود الدولية والداخلية**". الملتقى الدولي المحكم: الخصوصية في مجتمع المعلوماتية. ص٢٧.

الخاتمة:

يعيش عالمنا العصري تجدداً وتطوراً غير مسبق يتسم بالسرعة والتغير المستمر في طرق التواصل المختلفة، سواءً كانت على الصعيد الاجتماعي، التجاري، الحكومي او الدولي. مما أدى الى خلق تهديدات لجوانب أخلاقية من هوية الفرد، كالخصوصية والكرامة والاحترام. حيث إن هيكل منصات التقنية التي تقدم خدمات للفرد أصبح معتمداً بشكل رئيسي على جمع ومعالجة البيانات الشخصية للأفراد، مما عمل على وضع هذه البيانات الشخصية تحت خطر الانتهاك من خلال السرقة او الانتحال او المتاجرة او الاستعمال المسيء، الذي يهدد خصوصية الفرد. الا أن هذا النوع من الخصوصية تميز بخصائص مختلفة عن مفهوم الخصوصية خارج المنصات الالكترونية، ويتطلب بناءً على ذلك معاملة قانونية خاصة تراعي جوانبه المتفردة. ويتناول الجزء الأول من هذا البحث على أهمية بيان الفرق بين المفهوم التقليدي للخصوصية وبين مفهوم الخصوصية المعلوماتية المتجدد، من خلال معاينة نشأة كلاً من هاذين المفهومين وتحليل الخط الزمني لتطورهما.

ومع انتشار مفهوم الخصوصية المعلوماتية، أصبح حتميا على المجتمع الدولي التدخل قانونياً والاعتراف بهذا المفهوم واهمية التعامل معه كعنصر جديد مميز ومنفصل عن مفهوم الخصوصية التقليدي. أي أن الاتفاقيات الدولية التي اشارت الى حماية خصوصية وكرامة الانسان ليست كافية وشاملة لما يتطلب من حماية انتهاك الخصوصية المعلوماتية. وهذا ما يتناوله الجزء الثاني، من تحليل الخط الزمني للموقف الدولي تجاه توفير الحماية للحق في الخصوصية المعلوماتية والتحديات التي تواجه، إضافة الى إعادة النظر في فعالية دور الاتفاقيات الدولية في تقديم المفاهيم الجديدة للمجتمع الدولي، والمساهمة في تشجيع الدول على التعاون الدولي نحو الجرائم التي تتطلب تعاوناً دوليا كمعظم الجرائم الالكترونية. وفي الجزء الثالث من البحث، تم تحليل الموقف القانوني العام في مجابهة انتهاك الحق في

الخصوصية المعلوماتية. من خلال معاينة النصوص القانونية الدولية المعنية بتوفير الحماية للحق في الخصوصية المعلوماتية وبيان المعادلة بين الايجابيات والسلبيات التي فرضها الكيان القانوني الدولي تجاه توفير الحماية لهذا الحق.

النتائج:

-استنتج البحث أن دور التقنية في حياة الفرد أصبح حتميا لا مفر منه، وأنه أصبح من اللازم مواكبة هذا التطور اجتماعيا وقانونيا لما يترتب عليه من تحديات تهدد عناصر أساسية من حياة الفرد كخصوصيته.

-للجرائم الالكترونية طبيعة خاصية ومميزة عن بقية الجرائم العادية، مما يتطلب حماية قانونية خاصة تناسب هذه المميزات الخاصة.

-أن اغلب منصات التقنية الحديثة تعتمد على قواعد جمع البيانات الشخصية للمستخدمين ومعالجتها كإحدى مهامها الرئيسية.

-توجهات منصات التواصل الاجتماعي الحديثة نحو التسويق الالكتروني من خلال الخوارزمية التي تسمح باستخدام البيانات الشخصية المدخلة من قبل المستفيد، هي احدى أخطر مهددات الخصوصية المعلوماتية للفرد.

-دور الاعتراف القانوني بالخصوصية المعلوماتية في تطوير وتحسين الحماية القانونية المتوفرة لها.

-أن توحيد المفهوم القانوني للخصوصية المعلوماتية على الصعيد الدولي يكمن في تعاون الدول على تحسين تشريعاتها الداخلية لتواكب تطوير القوانين المنظمة للعالم الرقمي.

-دور الاتفاقيات الدولية في التعريف بالمفاهيم القانونية الحديثة كمفهوم الخصوصية المعلوماتية، وحث التعاون الدولي على الاعتراف بها والعمل على توفير الحماية القانونية اللازمة لها.

التوصيات:

-اوصي من خلال هذا البحث على تعزيز التعاون الدولي في توفير الحماية القانونية للخصوصية المعلوماتية من خلال الاستمرار في دعم انضمام الدول للاتفاقيات المعنية بذلك.

-العمل على توحيد مفهوم الخصوصية المعلوماتية وما يشمله ذلك من جوانب متعلقة كطبيعة الجرائم التي تهدد هذا المفهوم.

-خلق قواعد قانونية تنظيمية لجميع المؤسسات التي يكون أساس عملها جمع البيانات الشخصية ومعالجتها.

-العمل على دعم المزيد من الدول في الاعتراف القانوني بالخصوصية المعلوماتية واهمية توفير الحماية لها.

-بناء هيكل دولي قانوني متناسق يقوم على مواكبة اخر التحديثات التقنية التي تخص عمليات جمع البيانات ومعالجتها.

-اصدار الاتفاقيات التي تشمل بنود واضحة وصريحة في تنظيم ومكافحة جميع ما يهدد الخصوصية المعلوماتية

قائمة المراجع:

رسائل علمية:

لامى، بارق منتظر عبد الوهاب. (٢٠١٧م). جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني: دراسة مقارنة. رسالة ماجستير. جامعة الشرق الاوسط. كلية الحقوق. الأردن.

مجلات علمية:

الشريف، شريفي. (٢٠١٦). مدى احترام الحق في الخصوصية في الحسابات الإلكترونية على الإنترنت. جامعة أدرار – مخبر القانون والمجتمع. مجلة القانون والمجتمع. ١٣٢ – ١١٤

جاسم، فادية حافظ. (٢٠١٩م). التعاون الدولي للحد من الجريمة المعلوماتية. مجلة كلية الحقوق. جامعة النهرين. المجلد ٢١العدد ٤. العراق

بحوث ومقالات:

الزهراني، يحيى بن مفرح. (٢٠١٣م). تحديات الأمن المعلوماتي في الشبكات الاجتماعية في المملكة العربية السعودية من منظور قانوني. اتحاد الجامعات العربية – جمعية كليات الحاسبات والمعلومات. المجلة العربية الدولية للمعلوماتية. ١٢ – ١

العبيدي، أسامة بن غانم. (٢٠١٥م). الجهود الدولية لمكافحة الجرائم المعلوماتية. مجلة الحقوق. جامعة الكويت – مجلس النشر العلمي. مج٣٩، ع٤. ١١٣-١٥٦.

جديد، صبرينة. (٢٠١٨) الحماية القانونية للحق في الخصوصية المعلوماتية. مجلة التواصل في العلوم الانسانية والاجتماعية. جامعة عنابة مج٢٤، ع٢. ١٤٥-١٢٣.

خاطر، شريف يوسف حلمي. (٢٠١٥م). حماية الحق في الخصوصية المعلوماتية: دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا. مجلة البحوث القانونية والاقتصادية. جامعة المنصورة كلية الحقوق. ع٥٧. ١-١٧٠.

زينب، الضناوي. (٢٠١٩). الحماية القانونية للخصوصية على الانترنت في ظل الجهود الدولية والداخلية. الملتقى الدولي المحكم: الخصوصية في مجتمع المعلوماتية. مركز جيل البحث العلمي. طرابلس ٣٧-٢٣.

سامح، التهامي. (٢٠١٨). نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها: دراسة في القانون الاماراتي. مجلة البحوث القانونية والاقتصادية. جامعة المنصورة – كلية الحقوق ص٦٢٤-٦٣٢.

سلمان، عودة يوسف. (٢٠١٧). الجرائم الماسة بحرمة الحياة الخاصة التي تقع عبر وسائل تقنية المعلومات الحديثة، جامعة المستنصرية، كلية الرافدين– قسم القانون المجلد ١، العدد ٢٩-٣٠، الصفحات ١-٣٠.

سلمودي، رزق. (٢٠١٧م). الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي. الجامعة العربية الأمريكية – عمادة البحث العلمي. مجلة الجامعة العربية الأمريكية للبحوث. ٣٣ – ١

عائشة بن قارة، مصطفى. (٢٠١٦). الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية القانونية. مجلة الفقه والقانون. المجلد ٢، العدد ٦، الصفحات ٢٧٢-٢٨٩.

المراجع الإنجليزية:

"What is a Privacy Policy". Australian Government, office of the Australasian Information Commissioner.

Baiden, J. E. (2011). Cyber Crimes. *Available at SSRN 1873271*.

Beigi, G., & Liu, H. (2018). Privacy in social media: Identification, mitigation and applications. *arXiv preprint arXiv:1808.02191*.

Ghareb, M. I., & Sedeeq, F. M. Electronic Crimes And The International Community Legislation: Comparative Analytical Study.

Gritzalis, D., Kandias, M., Stavrou, V., & Mitrou, L. (2014). History of information: the case of privacy and security in social media. In *Proc. of the History of Information Conference* (pp. 283-310).

Jaishankar, K. (2007). Establishing a theory of cybercrimes. *International Journal of Cyber Criminology*, *1*(2), 7-9.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, *4*(4), 61-71.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New media & society*, *16*(7), 1051-1067.

Michael S. Josephson, Miller: The Assault on Privacy, 69 Mich. L. Rev. 1389 (1971). Available at: https://repository.law.umich.edu/mlr/vol69/iss7/6

Ramdinmawii, E., Ghisingh, S., & Sharma, U. M. (2014). A study on the cyber-crime and cyber criminals: A global problem. *International Journal of Web Technology*, *3*, 172-179.

Rollenhagen, Luisa."Alan Westin is the father of data privacy law". Osano. January 15, 2021

Schlosser, A. E. (2020). Self-disclosure versus self-presentation on social media. *Current opinion in psychology*, *31*, 1-6.

Such, J. M., & Criado, N. (2018). Multiparty privacy in social media. *Communications of the ACM*, *61*(8), 74-81.

Weber, R. H. (2015). The digital future–A challenge for privacy? *Computer Law & Security Review*, *31*(2), 234-242.

Xie, W., & Kang, C. (2015). See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior*, *52*, 398-407

Zheleva, E., & Getoor, L. (2009, April). To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *Proceedings of the 18th international conference on World wide web* (pp. 531-540).

Treaties & Conventions:

International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966

Treaties and International Agreements on Privacy & Data Protection. International and Foreign Cyberspace Law Research Guide. Georgetown law library

Vienna Convention on the Law of Treaties, Done at Vienna on 23 May 1969. Entered into force on 27 January 1980. United Nations, Treaty Series, vol. 1155

Official Websites:

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, available at: https://www.refworld.org/docid/3ae6b3b04.html [accessed 8 September 2021]

European Court of Human Rights, Europe's Human Rights Watchdog. Accessed At https://www.europewatchdog.info/en/council-of-europe/

Online Websites:

7 Principles of Privacy by Design, Internet Privacy Guy. Nov 20, 2017. Accessed At https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce

Cases:

Collection of Personal Data Cases, European Court of Human Rights.

The Catt that got the cream – retention of data concerning peaceful protestor was an unlawful interference with article 8, UK Police Law Blog. Serjeants' Inn Chambers.