ISSN:2335-1462 مجلة القانون والمجتمع eISSN: 2600-609X
المجلد: 12 العدد: 02 السنة: 2024 الصفحة: 207 - 222

عنوان بروتوكول الأنترنت وعلاقته بالبيانات الشخصية عبر مواقع التواصل الاجتماعي

Internet Protocol Address and its Relationship to Personal Data on Social Media Sites

1- عبد القادر بهادي*
كلية الحقوق والعلوم السياسية
جامعة أحمد درايعية أدرار - الجزائر.
Bahaddi.abdelkader@univ-adrar.edu.dz

2- عبد القادر الصادق
كلية الحقوق والعلوم السياسية
جامعة أحمد درايعية أدرار - الجزائر.
Saddek7@gmail.com

1- Abdelkader Bahaddi
Faculty of law and Political Science
University of Ahmed Draia - Adrar- Algeria
Bahaddi.abdelkader@univ-adrar.edu.dz

2- Abdelkader Saddek
Faculty of law and Political Science
University of Ahmed Draia - Adrar- Algeria
Saddek7@gmail.com

تاريخ الاستلام: 2024/11/05 تاريخ القبول: 2024/11/ 18

ملخص باللغة العربية:

تتناول هذه الدراسة عنوان بروتوكول الانترنت باعتباره بطاقة التعريف لأي جهاز له اتصال بشبكة الانترنت مثل الهواتف، الكمبيوتر، الطابعة وغيرها من الأجهزة وعلاقتة بمواقع التواصل الاجتماعي، فبواسطة عنوان بروتوكول الانترنت يمكننا معرفة مالك الجهاز والمعلومات الخاصة به، وكذا المواقع التي تم تصفحها والأكثر من ذلك معرفة المعلومات التي تحتويها وهنا نكون أمام انتهاك للخصوصية.

الكلمات المفتاحية: مواقع التواصل الإجتماعي؛ البيانات الشخصية؛ عنوان بروتوكول الانترنت؛ الأمن السيبيراني.

ABSTRACT:

This study deals with the Internet Protocol address as theidentification card for any device connected to the Internet such as phones, computers, printers and other devices and its relationship to social networking sites. Through the Internet Protocol address, we can know the owner of the device and its private information, as well as the sites that have been browsed and more than that, know the information they contain. Here we are faced with a violation of privacy

Keywords: *Social media ; Personal data; IP address; Cyber security.*

* المـؤلف المرسل.

مقدمـــة:

إن التطور في المجال التكنولوجي والاتصالات الذي شهده العالم والذي كان له تأثيرا ظاهرا على الخصوصية من حيث انتهاكها، فبظهور الانترنت والتي أصبحت الآن شريان الحياة بالنسبة للفرد أو للمؤسسة أو الشركة، كما لها من أهمية بالغة في ظهور مواقع التواصل الاجتماعي ولما وصلت له من تحديثات، فأصبح بواسطتها إمكانية التواصل بين المستخدمين عبر العالم وكذا التسويق وغيرها من المزايا.

كما يعتبر عنوان بروتول الانترنت من أهم الوسائل التي من خلالها يتم تحديد هوية مستخدم الانترنت عامة، وكذا التطبيقات والمواقع التي تعمل بها خاصة، ومن هنا تبرز أهمية دراسة الموضوع، للوقوف على علاقة عنوان بروتكول الانترنت بالخصوصية عبر مواقع التواصل الإجتماعي.

ولمحاولة البحث في الموضوع نثير الإشكالية التالية: ما علاقة عنوان بروتوكول الانترنت بالبيانات الشخصية لمواقع التواصل الإجتماعي ؟، وما مدى تأثيره عليها ؟

وللإجابة على هذه الإشكالية انتهجنا المنهجين المنهج الوصفي والمنهج التحليلي، حيث تم الاعتماد على خطة متكونة من مبحثين؛ يضم المبحث الأول: مدى تأثير عنوان بروتكول الانترنت على خصوصيات مواقع التواصل الاجتماعي، أما المبحث الثاني: البعد القانوني بعد الكشف عن البيانات الشخصية لمستخدم مواقع التواصل الاجتماعي بواسطة عنوان بروتكول الانترنت.

المبحث الأول: مدى تأثير عنوان بروتكول الانترنت على خصوصيات مواقع التواصل الاجتماعي.

إن لهذا العنوان (address IP) أهمية كبيرة في شبكة الانترنت فهو الوسيلة التي بواسطتها يستطيع التعرف على المستخدم للأجهزة المتصلة بالانترنت، إذ يمكن بواسطته تحديد إسم النطاق، وكذا تحديد اسم الشركة أو من قام بتسجيله، وذلك عن

طريق نظام أسماء المنظمات وتحديد موقعها"[1]، كما يتم تحديد المواقع التي تمت زيارتها، ونستثني خلال هذا البحث مواقع التواصل الإجماعي وعلاقتها بهذا العنوان فمن هنا تبدأ خطورته وانعكاساته على الخصوصية بصفة عامة وعلى البيانات الشخصية المنتشرة عبر هذه المواقع بصفة خاصة، كما له خصائص عديدة ومتعددة نذكر منها على سبيل المثال لا الحصر:

- هو عبارة عن وسيلة لتحديد هوية المستخدم للجهاز المتصل بالانترنت.
- يحدد العناوين والمواقع التي تم البحث عنها في محركات البحث المتعددة وذلك لأن هذه المحركات تقوم بحفظ بيانات عنوان بروتكول الانترنت تلقائياً، حيث يسهل التعرف على المستخدم .
- يحدد الجهة التي يستخدم فيها الشخص شبكة الانترنت.

إذن فمن خلاله يتم التعرف على كافة أنواع السلوك للمستخدمين عبر الانترنت عامة، بما في ذلك مستخدمي مواقع التواصل الاجتماعي خاصة، وذلك بانتهاك خصوصياتهم، وهذا ما سيتم التطرق له خلال هذا البحث حيث ستتم دراسة إجراءات اقتناء الأجهزة المتصلة بالانترنت ومدى الالتزام بكشف الهوية، في المطلب الاول، أما المطلب الثاني ندرس خلاله خصوصيات مواقع التواصل الاجتماعي وتأثيرها بعنوان بروتوكول الأنترنت

المطلب الأول: إجراءات اقتناء الأجهزة المتصلة بالانترنت ومدى الالتزام بكشف الهوية.

تعتمد الانترنت أساساً على البروتوكولات فهي التي تتحكم فيها، "ولقد عرفها كل من Christofol.H و Richir.S على أنها التكنولوجيا المرتكزة على بروتوكولات IP-TCP، فالأول بروتوكول التحكم في الارسال، أما الثاني فهو بروتوكول التحكم في الانترنت"[2].

1 علي وهبي ديب، الحق في حماية البيانات الشخصية، منشورات الحلبي الحقوقية، بيروت–لبنان، ط1، 2023، ص 322.

2 لحمر عباس، البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال، دار خومة للطباعة والنشر والتوزيع، الجزائر، 2018، ص 50.

ويعرف عنوان بروتكول الانترنت بأنه" عبارة سلسلة أرقام، تختلف من جهاز لآخر والتي تميز الجهاز عن غيره من الأجهزة الأخرى المتصلة بالأنترنت، مثل جهاز الكومبيوتر أو الطابعة أو الهاتف"[1].

ومن هنا نجد إنه هو الذي يمكن المستخدم للوصول إلى الانترنت، كما انه المسؤول عن كشف البيانات الشخصية للمستخدم، فبواسطته يمكن التعرف على صاحب الجهاز وكذا مكان تواجده.

وأكدت دراسة مكتب مفوضية الخصوصية في كندا "أنه من خلال عنوان بروتوكول الانترنت يتم التعرف على عدد الزيارات التي قام بها الشخص لمواقع معين على شبكة الأنترنت"[2].

نحاول في هذا المطلب التطرق إلى: إجراءات شراء الأجهزة المتصلة بالانترنت في الفرع الأول، أما الفرع الثاني فيتم التطرق إلى: إلزامية الكشف عن البيانات الشخصية عند شراء الأجهزة المتصلة بالانترنت.

الفرع الأول: إجراءات شراء الأجهزة المتصلة بالانترنت.

من المعلوم أن شراء أي جهاز كانت له علاقة واتصال بالانترنت مثل هاتف محمول أو كومبيوتر أو أجهزة الاتصال السلكي أو اللاسلكي وغيرها من الأجهزة، عند شرائه يستلزم إبرام عقد لشرائها، فالشركات التجارية التي تقوم ببيع مثل هذه الأجهزة تقوم بملأ بيانات المشتري للجهاز وتتكون هذه البيانات من إسمه، تاريخ ميلاده، عنوانه، رقم هاتفه، والأبعد من ذلك تحتفظ بنسخة من بطاقته التعريفية، وهو الحال كذلك بالنسبة لشرائح الهواتق النقالة والتي تعتبر وسيلة للإتصال بالانترنت كذلك، وهنا يجد المشتري نفسه أمام خيارين إما شراء الجهاز والكشف عن بياناته الشخصية أو عدم إقتنائها، فيجد نفسه مجبراً لا مخيراً لشراء ذاك الجهاز لأهميته

1 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، البعد الحقوقي لعنوان بروتوكول الأنترنت وتأثيره على الخصوصية، مجلة كلية القانون الكويتية العالمية، الكويت، السنة الثامنة، العدد 4، العدد التسلسلي 32، ديسمبر 2020م، ص 290.

2 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، نفس المرجع، ص 289.

البالغة في حياتنا اليومية، والتي أصبحت تعتمد على الرقمنة في جل مجالات الحياة، إن لم نقل كلها.

الفرع الثاني: إلزامية الكشف عن البيانات الشخصية عند شراء الأجهزة المتصلة بالانترنت.

إذا كان من الضرورة بمكان إلزامية الكشف عن البيانات الشخصية عند شراء الأجهزة المتصلة بالانترنت، هنا يترتب على عاتق الشركات التجارية التي تعمل في مجال بيع هذه الأجهزة التحلي بروح المسؤولية وتحملها، للحفاظ على هذه البيانات وعدم انتهاكها والتلاعب بيها كتداولها وبيعها وغيرها من الانتهاكات، ولأن الدستور الجزائري كباقي دساتير دول العالم كرس حماية الحياة الخاصة عامة ومن بينها الخصوصيات للأفراد، كما أن المشرع الجزائري سن قوانين تنظم وتحمي البيانات الشخصية من الإنتهاك، حفاظا على كرامة الإنسان وخصوصياته.

المطلب الثاني: خصوصيات مواقع التواصل الاجتماعي وتأثيرها بعنوان بروتوكول الأنترنت.

كما تمت الإشارة إليه سابقاً فإن الحق في الخصوصية مكفول، تكفله الدولة، والتعدي عليه يعتبر جريمة يعاقب عليها القانون، واستعمال الأجهزة المتصلة بالانترنت لها خصوصية بالنسبة للمستخدم وهذا حق مشروع، ومن بين هذه الأجهزة نركز الضوء على أجهزة الإتصال الحديثة والتي تضم مواقع التواصل الاجتماعي الذي يضم العديد من خصوصيات المستخدمين، فنحاول دراستها من خلال فرعين، الفرع الأول يضم: أبعاد الخصوصية عبر هذه المواقع، اما الفرع الثاني: المشروعية في الكشف عن البيانات الشخصية عبر هذه المواقع باستعمال عنوان بروتوكول الأنترنت.

الفرع الأول: أبعاد الخصوصية عبر مواقع التواصل الإجتماعي.

يجد المشتري للأجهزة المتصلة بالانترنت نفسه مجبراً على الكشف عن بياناته الشخصية للشركة التجارية التي تبيع هاته الأجهزة، ومن هنا فقد تصبح تلك البيانات عرضة للإنتهاكات كما قلنا سابقاً، بواسطة القرصنة واستعمال أساليب

تكنولوجية متطورة، ونحصر دراستنا على أجهزة الإتصال المتطورة، التي تحمل تطبيقات مواقع التواصل الاجتماعي، من هواتف ذكية وأجهزة الإعلام الآلي المحمولة والثابتة.

وكما يعلم العام والخاص مدى إحتواء هذه المواقع من خصوصيات لمستعمليها، حيث بإمكان عنوان بروتوكول الأنترنت الوصول إليها من خلال الجهاز عند إتصاله بالأنترنت، ويكون ذلك إما بطرق مشروعة في حالة التحري التي أجازها المشرع وفي حدود ضيقة، أو بطرق غير مشروعة والمتمثلة في القرصنة أو باستعمال التطبيقات الذكية، وحرصاً على احترام الحق في الخصوصية أوجد المشرع الجزائري قانون خاص ينظم ويحمي الأشخاص في مجال معالجة المعطيات، وهو القانون 18-07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي"[1]، حيث جاء في مضمون المادة الثانية منه، على وجوب احترام الكرامة الإنسانية، وعدم المساس بحقوقهم من سمعة وشرف.

والمعلوم أن المستخدم للانترنت عامة ومستخدم مواقع التواصل الاجتماعي خاصة، له الحق في حماية خصوصياته من كل الوسائل التي تهددها، ومن بينها عنوان بروتوكول الانترنت، الذي يعتبر مهددا خطيرا للبيانات الشخصية.

أما الإعتداء على الخصوصية باستخدام البيانات الشخصية بطريقة غير قانونية أي غير مشرعة والمتمثل في العديد من الجرائم والأعمال الممارسة من طرف الفرد أو الجهات الحكومية، والمتمثلة على سبيل المثال في الإبتزاز، التشهير، التنصت، وذلك بواسطة اختراق الأنظمة المعلوماتية للتمكن من الوصول إليها بدون سبب شرعي يتيح ذالك[2].

إلا إن هناك بالمقابل تقنية تسمى قي بي أن VPN، هذه التقنية تسمح لمستخدمي الأنترنت بإخفاء هوياتهم وبياناتهم الرقمية عند إتصال أجهزتهم بشبكة

1 القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

2 منى الأشقر جبور، ومحمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ط1، 2018، ص 22.

الانترنت وذلك حفاظاً عليها من إنتهاكها من طرف مجرمي هذه شبكة الأنترنت، والمعروف أن مزود خدمة الانترنت "ISP" الذي يعتبر العنصر المحوري بين المستخدم وشبكة الأنترنت وما تحويه من مواقع مختلفة، فهو على دراية تامة بجميع البيانات الرقمية الخاصة بالمستخدمين لها والمتصلين عن طريقه، كما له القدرة على اعتراض جميع هذه البيانات فيمكنه مشاهدتها، وله القدرة على الإحتفاظ بها لمدة معينة، ليستعملها أو ليتعاون مع الجهات القضائية أو الأمنية إذا تطلب الأمر ذلك؛ أي في حالة وجود رخصة شرعية والتي سيتم التطرق لها بالتفصيل لآحقاً.

فمن إجل هذا يقوم معظم المستخدمين الذين لهم ذراية بالموضوع بتشفير بياناتهم وحتى إتصالاتهم عبر مواقع التواصل الاجتماعي، حتى لا يتمكن مزودي خدمة الأنترنت من الإطلاع عليها"[1].

ومن هنا نجد أن للخصوصية في استعمال الأجهزة المتصلة بالانترنت أبعاد متمثلة في الانتهاكات للبيانات الشخصية والمعلومات الخاصة لمستخدم مواقع التواصل الاجتماعي خاصة، والمواقع الأخرى والعديدة المنتشرة عبر شبكة الأنترنت.

الفرع الثاني: المشروعية في الكشف عن البيانات الشخصية عبر مواقع التواصل الإجتماعي باستعمال عنوان بروتوكول الأنترنت.

إن الإعتداء على البيانات الشخصية يعد جريمة يعاقب عليها المشرع، إلا أنه توجد استثناءات لهذا الأمر، إذ يمكن ذلك في ظروف استثنائية؛ أي عندما تكون المصلحة العامة أو حياة شخص آخر معرض للخطر، كما يستثنى في حالة الاستخدام الغير مشروع للأجهزة المتصلة بالأنترنت، مثال ذالك اتصلات مشبوهة من مواقع التواصل الاجتماعي، أو التحري عن معلومات لمستخدم مشبوه، أو تقصي وتتبع آثار مجرمين، أو التخطيط لجريمة، إلا أن هذا التحري لزم أن يبنى على التوازن، حيث إنه لا يكون بصفة مطلقة بل مبني على الإحترام، وأن يتماشى وطبيعة الإستثناء، أما في إطار الشرعية فهو مكفول كفالة تامة"[2].

1 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، المرجع السابق، ص 289.

2 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، نفس المرجع، ص 304.

بحيث يكون التحقيق والكشف عن البيانات الشخصية بطرقة مشروعة ومن طرف أشخاص معينن مثل ضباط مؤهلين أو أفراد من السلطة القضائية المختصة، وقد حددها ما جاء من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المادة 5 منه[1]، كما أوجد المشرع هيئة وطنية مختصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحته"[2]، وهذا ما نصت عليه المادة 13 من نفس القانون.

ومن هنا نجد أن المشروعية للكشف عن البيانات الشخصية للمستخدم عبر أي موقع في شبكة الأنترنت، يكون في إطار ضيق ومراقب من قبل الجهات الوصية وذلك حفاظا على مبدأ حق حماية الخصوصية

المبحث الثاني: البعد القانوني بعد الكشف عن البيانات الشخصية لمستخدم مواقع التواصل الاجتماعي بواسطة عنوان بروتوكول الانترنت.

إن المجتمعات التي تتبنى منهج الديمقراطية، تعتبر حق حماية الخصوصية ركن أساسي من أركان قيامها، وهذا ركن جوهري لحفظ كرامة الانسان، كما أن ديننا الحنيف أكد على ذلك في القرآن الكريم، في سورة الحجرات"[3]، وجاء مصطلح التجسس في الآية بمعنى التتبع لخصوصيات الناس.

لذا يعتبر التعدي على الخصوصية خط أحمر ويعاقب عليه القانون، إلا أنه يمكن الكشف عن البيانات الشخصية لشخص معين إذا كان الأمر ضروري لتحقيق غرض مشروع ومنصوص عليه في التشريع، كما لزم أن يتوفر مبدأ التناسب مع الغرض المنشود، كما تم التطرق له سابقاً.

وبما أن عنوان بروتكول الانترنت من بين أهم التقنيات التي تحوي خصوصيات مستخدم أي جهاز متصل بالأنترنت، وما يحويه من تطبيقات تعج

1 القانون 09-04 المؤرخ في 5 غوشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

2 المادة 13، من نفس القانون.

3 سورة الحجرات، الآية 12: ﴿ يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ ۖ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا ۚ...﴾" صدق الله العظيم.

بالبيانات الشخصية لمستعمليها، ونخص بالذكر مواقع التواصل الاجتماعي، التي تعرف بأنها مواقع إلكترونية إجتماعية متاحة لمستخدمي الأنترنت وتسمح للتواصل فيما بينهم"[1]، فيمكن خلالها تبادل الآراء وتداول الأخبار، والنشر والتفاعل عبر صفحاتها، بين المستخدمين، حيث لا تتطلب هذه المواقع لفتح حساب فيها لأي شروط معينة، سوى إدخال بياناتك الشخصية فقط.

فمن خلال هذا المبحث نتطرق إلى مسؤولية المتتبع لهذا العنوان وانتهاك خصوصيات مستخدمي مواقع التواصل الإجتماعي في المطلب الأول، أما في المطلب الثاني: مسؤولية مستخدم الجهاز بطريقة غير مشروعة وانتهاك خصوصيات مستخدمي مواقع التواصل الاجتماعي.

المطلب الأول: مسؤولية المتتبع لعنوان بروتكول الأنترنت وانتهاك خصوصيات مستخدمي مواقع التواصل الإجتماعي.

يعد تعقب عنوان بروتكول الانترنت جريمة يعاقب عليها القانون، إلا إذا كان لهذا التتبع شرعية قانونية، أو لمصلحة عامة، فإنه في هذه الحالة يجوز، أما ما خلاف ذلك فيرتب مسؤولية لمن تتبع هذا العنوان لأي شخص.

فمن خلال هذا المطلب نحاول التطرق إلى المسؤولية التعاقدية لمتتبع عنوان بروتوكول الانترنت في الفرع الأول، أما في الفرع الثاني: المسؤولية التقصيرية لمتتبع هذا العنوان.

الفرع الأول: المسؤولية التعاقدية لمتتبع عنوان بروتوكول الانترنت.

لما نشير إلى المسؤولية التعاقدية نكون أما عقد قد ابرم بين طرفين، وهنا المقصود إن الاعتداء قد تم من قبل مزودي خدمة الانترنت أو خدمة الاتصال بالشبكة وما تحويه من مواقع، وهذا النوع من العقود يتسم بالسرية وحماية خصوصية المشترك التي قد أدلى بها خلال انشاء العقد.

1 صادق عباس مصطفى، الإعلام الجديد مفاهيم وسائل وتطبيقات، دار الشروق للنشر والطباعة، الأردن، 2018، ص 216.

فتقوم المسؤولية التعاقدية لما يتم الانتهاك والتتبع لعنوان بروتوكول الانترنت من طرف مزودي الخدمة، إذ أن عدم تحقق النتيجة المطلوبة للمستخدم والذي يعد دائنا في العلاقة التعاقدية وهي الحفاظ على بياناته الشخصية من الانتهاك، "ولا تستطيع هذه الجهات التهرب من المسؤولية إلا في حالة إثبات إن الأمر قد تم بسبب خارج عن الإرادة إما بقوة قاهرة أو بسبب أجنبي، مثلما أن يكون الإنتهاك قد حصل بسبب مشكلة تقنية[1]، كما جاء في الامر 75-58، المتضمن القانون المدني الجزائري، فيما يخص المسؤولية التعاقدية، في المادة 124 منه[2]، فمن خلال نص المادة نجد أن الضرر الذي أحدث بسبب خطأ الغير، يلزمه تعويض المتضرر.

الفرع الثاني: المسؤولية التقصيرية لمتتبع عنوان بروتوكول الانترنت.

إن المسؤولية التقصيرية صورة من صور المسؤولية المدنية، ونكون أمام هذه المسؤولية في حالة تتبع عنوان بروتوكول الأنترنت، إذا قام شخص ثالث غير المسؤول عنه، بالوصول إليه، كأن يكون مثلا مستخدم آخر للشبكة، حيث يقوم هذا الأخير مستخدماً هذه التقنية التي وصل إليها بتقصير من المسؤول، منتهكاً للبيانات الشخصية للمعني ومسبباً له ضرراً.

فيمكن أن يكون فعل الفاعل متعمداً كشف بيانات المستخدم من خلال عنوان بروتوكول الانترنت، كما يمكن أيضاً أن يتم مباشرةً أو تسبباً، فالمتحكم في المعلومات يكون هو من إحداث الضرر بالمستخدم حين، وقد يتسبب بإحداث الضرر عند توسطه، مثال ذلك كأن يكون معالج المعلومات قد تحصل على بيانات شخصية للمستخدم بواسطة هذا العنوان، وأهملها أو قام بتخزينها لمدة أطول، مما جعلها تصل إلى شخص ثالث أين قام هذا الأخير بانتهاكها[3].

1 محمد سليمان الأحمد، الخطأ وحقيقة أساس المسؤولية المدنية في التشريع العراقي، مكتب التفسير، أربيل، 2008، ص 15.

2 الامر 75-58، المؤرخ في 26-09-1975، المتضمن القانون المدني الجزائري، المعدل والمتمم.

3 محمد سليمان الأحمد، المرجع السابق، ص 59.

وهذا ما تمت معالجته في القانون 18-07، من المادة 43 منه[1]، حيث أوضح المشرع من خلالها إن قيام المسؤولية التقصيرية على مقدم الخدمة، تكون بمجرد عدم أخذ تدابير الأمان في حالة وصول الغير للبيانات الشخصية وانتهاكها.

المطلب الثاني: مسؤولية مستخدم الجهاز بطريقة غير مشروعة وانتهاك خصوصيات مستخدمي مواقع التواصل الإجتماعي.

تعتبر شبكة الأنترنت فضاء خصب لتفشي جل الأعمال غير المشروعة من ابتزاز وتشهير ونشر للرذيلة والصور والمواقع الإباحية، المنتشرة عبر تطبيقات مواقع التواصل الاجتماعي المختلفة، وذلك ظناً من هؤلاء المستخدمين أنه لا رقابة عليهم وأن استخدامهم لأجهزتهم بطريقة غير مشروعة يستحيل التعرف عليهم وكشف هويتهم، لكن هيهات، فالسلطات الأمنية والقضائية وضعت حاجزاً منيعاً لكل من سولت له نفسه المساس بالمصلحة العامة وكذا للسكينة العامة، أو خرق الأمن والنظام العام للبلاد، وهذا حال باقي دول العالم، فمن خلال هذا المطلب سنتطرق إلى مسؤولية مستخدم الجهاز بطريقة غير مشروعة في حالة خرق الأمن والنظام العام في الفرع الأول، أما الفرع الثاني ندرس المسؤولية في حالة سوء الأخلاق والآداب العامة.

الفرع الأول: مسولية مستخدم الجهاز بطريقة غير مشروعة في حالة خرق الأمن والنظام العام عبر المواقع.

إذا كان الكشف عن عنوان بروتوكول الانترنت يعتبر انتهاكاً لحق الخصوصية وهذا هو الأساس، إلا أنه يمكن القول أن الكشف عنه جائز في حالة المصلحة العامة أو منع الضرر، والجرائم الإلكترونية، ومن المعلوم كما قلنا سابقاً أن

1 المادة 43، القانون 18-07: "إذا أدت معالجة المعطيات ذات الطابع الشخصي في شبكات الإتصالات الإلكترونية المفتوحة للجمهور إلى إتلافها أو ضياعها أو إفشائها أو الولوج غير المرخص إليها، يعلم مقدم الخدمات فوراً السلطة الوطنية والشخص المعني إذا أدى ذلك إلى المساس بحياته الخاصة، مالم تقرر السلطة الوطنية أن الضمانات الضرورية لحماية المعطيات قد تم اتخاذها من قبل مقدم الخدمات".

معظم الجرائم تتم عبر الفضاء الإفتراضي في مواقع التواصل الإجتماعي خصوصاً، فإذا تم تتبع عنوان بروتوكول مستخدم لهذه المواقع يحاول المساس بالأمن والنظام العام، لكن هذا التتبع يسبقه ترخيص، ويكون هذا الترخيص من الجهات المعنية بذلك وهذا ما جاء في القانون القانون 18-07، من المادة 17 منه[1]، فمن مضمون المادة يتبين لنا أن المشرع الجزائري أولى أهمية بالغة للحفاظ على حق الخصوصية حين أخضع المعالجة في حالات استثنائية إلى ترخيص مسبق، فهذا الترخيص هو الذي يقرر إذا كان الأمر يستوجب المعالجة أم لا.

ومن هنا نستشف أن نظام الترخيص المسبق له دلالة على احترام مبدأ الخصوصية لمستخدمي شبكة الأنترنت عامة والمواقع الاجتماعية خاصة، حتى لا يكونوا عرضة للإنتهاك حتى من طرف الجهات الأمنية.

ومن الامثلة الحية فيما يخص هذا الشأن نذكر على سبيل المثال الواقعة التي حدثت في الهند؛ حيث حدث في موباي بالهند، خلال شهر فبراير 2011، تتبع الشرطة لصبي مفقود هرب من منزلهم، وكان ذلك باتباع فايسبوك الصبي بتقنية عنوان بروتوكول الانترنت[2]، فمن خلاله تم العثور على الطفل بعد تعقب أثره بواسطته.

الفرع الثاني: مسؤولية مستخدم الجهاز بطريقة غير مشروعة في حالة سوء الأخلاق والآداب العامة عبر المواقع.

نفس الشيء الذي ينطبق على مسولية مستخدم الجهاز بطريقة غير مشروعة في حالة خرق الأمن والنظام العام ينطبق في حالة سوء الأخلاق والآداب العامة، لأنه يعتبر مساس بوحدة الوطن وبحقوق وحريات المواطنين، فكل من يقوم بفعل الذم والسب وكذا زرع الفتنة، ونشر الرذيلة وبالخصوص في مواقع التواصل الاجتماعي

1 المادة 17 من القانون 18-07: "تقرر السلطة الوطنية إخضاع المعالجة المعنية لنظام الترخيص المسبق عندما يتبن لها، عند دراسة التصريح المقدم لها، أن المعالجة المعتزم القيام بها تتضمن أخطار ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص".

2 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، المرجع السابق، ص 312.

التي تعتبر فضاء لإنتشار مثل هذه الأفعال المشينة من طرف مستخدمين لهم إنطباعات سيئة، فيكون حينئذ أمام مسؤولية الاستعمال الغير مشروع للجهاز الخاص بهم والذي تم إستعماله، ويتم الكشف عنه من خلال تتبع هذا العنوان الخاص به.

تحتوي الهند أكثر مستخدمي الانترنت في العالم، حيث حصلت عدة وقائع أدت لضرورة التحري عن بعض مستخدمي الشبكة وذلك من خلال الإستعانة بعنوان بروتكول الأنترنت، ففي حادثة وقعت في شهر ماي من عام 2010، أين تم اعتقال ضابط في الشرطة في مدينة مومباي الهندية، حيث كان يوزع مواد إباحية للأطفال من خلال حاسوبه عبر مواقع التواصل، بعد أن نبهت الانتربول السلطات الهندية بأن الصور الإباحية كان يتم تحميلها من عنوان بروتوكول الانترنت الذي كان يستخدمه"[1]، فبواسطة هذا العنوان يختصر الجهد والوقت لمصالح الأمن المختصة وتكشف المخططات الإجرامية.

الخاتمة:

إن عنوان بروتوكول الانترنت يعتبر من بين إحدى الخصوصيات للفرد في البيئة الرقمية خلال اتصاله بالشبكة العنكبوتية؛ لأنه يحتوي على كل البيانات الشخصية المتعلقة بالمستخدم، كما يعتبر الفرد مجبراً لا مخيراً للإدلاء بها، وذلك من أجل اقتناء الجهاز والانتفاع به، لما له من أهمية بالغة في حياتنا اليومية، حيث أصبح من الضروريات التي تسهل حياة الفرد اليومية، باختصار الجهد والوقت، وفي جل المجالات المختلفة، وخاصة أجهزة الإتصال الحديثة والمتطورة، التي تتضمن عدة مواقع مختلفة تحوي العديد من البيانات الشخصية للمستخدم، ونخص بالذكر مواقع التواصل الاجتماعي، فمن هنا تبدأ رحلة المغامرة بالنسبة لتلك البيانات في فضاء الانترنت الذي يعتبر أرض خصبة للانتهاكات بطرق مختلفة وجد متطورة تتطور بتطور التكنولوجيا الحديثة، وأول خطر يترصد تلك البيانات هو خطر انتهاكها من طرف مزودي خدمة الانترنت أو محركات البحث المتعددة والمتطورة،

1 محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، المرجع السابق، ص ص 311-312.

وكذا مواقع الويب، بدأ من عنوان بروتول الأنترنت، فمن أهم النتائج والتوصيات التي استخلصت من هذه الدراسة مايلي:

النتائـــــج:

بالرغم من تشديد الحرص من طرف المشرع الجزائري وكافة تشريعات العالم على الحق في الخصوصية وحمايتها، إلا أن انتهاكها مازال مستمر، فالإعتماد على القواعد العامة ليس حلا، خاصة مع التطور السريع في مجال تكنولوجيا الإتصالات وشبكة الأنترنت التي لا تعرف للحدود الجغرافية معنى، ومن بين السبل التي تُتبع لإنتهاك البيانات الشخصية بالخصوص عبر مواقع التواصل الاجتماعي، هو تَتبع عنوان بروتوكول الأنترنت، حيث أصبحت البيانات الشخصية من أثمن البضاعة في السوق الرقمية، وأربح تجارة، ذلك لأهميتها في عدة مجالات منها التجارية والإقتصادية والإجتماعية وحتى السياسية، فبواسطتها يتم تحدد السلوكيات والحاجيات والمتطلبات الشخصية للمستخدم، كما أن لعنوان بروتوكول الأنترنت إيجابيات منها، اكتشاف المجرمين من خلال تتبع عنوانهم عبر الشبكة، والقضاء على الجريمة المنظمة والتصدي لها قبل حدوثها بواسطة السلطة القضائية والأمن السيبيراني.

التوصيـــات:

- ضرورة تشديد الرقابة والأمن من طرف السلطات المعنية على شبكة الأنترنت عامة لأنها تعتبر الفضاء الخصب لإنتهاك البيانات الرقمية لمستخدميها، وعلى مواقع التواصل الاجتماعي خاصة لأنها تعتبر الآن وسيلة ضرورية في حياة الفرد، نظراً لما تحتويه من إيجابيات، فهي تسهل متطلبات الحياة وتوفر الجهد، وتقدم خدمات جد متطورة، لذا كان لزاما توفير الأمن لمستخدميها.
- استحداث أمن سيبيراني متطور وتعزيز مهاراته ليتماشى ومتطلبات التطورات الراهنة على تكنولوجيا الاتصالات، وذلك لتضييق الخناق على المنتهكين للبيانات الشخصية عبر هذه المواقع.
- ضرورة سن قوانين ردعية من طرف المشرع، تحد من هذه الإنتهاكات، متماشية والتطور التكنولوجي لمواقع التواصل الإجتماعي.

- تحرك العالم بأسره لتفعيل الحماية اللازمة للبيانات الشخصية الرقمية على مستوى شبكة الأنترنت عامة، وعبر مواقع التواصل خاصة، للحد من الإنتهاكات لأن العالم كله أصبح قرية صغيرة، وذلك بسن إتفاقيات ومعاهدات دولية تحترمها كل دول العالم.
- تنمية فكر المستخدم لمواقع التواصل الاجتماعي، وتوعيته لخطورة انتهاك البيانات الشخصية، ذلك من خلال الإعلام والمحاضرات.

قائمة المراجع والمصادر:

أولاً- القرآن الكريم برواية ورش.

ثانياً- الكتب:

- لحمر عباس، البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2018.
- محمد سليمان الأحمد، الخطأ وحقيقة أساس المسؤولية المدنية في التشريع العراقي، مكتب التفسير، أربيل، العراق، 2008.
- منى الأشقر جبور،و محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، ط1، 2018.
- علي وهبي ديب،الحق في حماية البيانات الشخصية، منشورات الحلبي الحقوقية، بيروت، لبنان، الطبعة الأولى، 2023.
- صادق عباس مصطفى، الإعلام الجديد مفاهيم وسائل وتطبيقات، دار الشروق للنشر والطباعة، الأردن، 2018.

ثالثاً- المجلات العلمية:

- محمد سليمان الأحمد، وعبد الكريم صالح عبد الكريم، البعد الحقوقي لعنوان بروتوكول الأنترنت وتأثيره على الخصوصية، مجلة كلية القانون الكويتية العالمية، الكويت، السنة الثامنة، العدد 4، العدد التسلسلي 32، ديسمبر 2020.

رابعاً- النصوص القانونية:

- الأمر 70-58 المؤرخ في 1975/09/26، المتضمن القانون المدني الجزائري، المعدل والمتمم.

- القانون 18-07 المؤرخ في 10 يونيو 2018، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

- القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.