البُعد الحقوقي لعنوان بروتوكول الإنترنت «IP address» وتأثيره على الخصوصية: دراسة تحليلية في القانون المدني

أ. د. محمد سليمان الأحمد
أستاذ القانون المدني
كلية القانون، جامعة السليمانية، العراق
والأستاذ الزائر، جامعة الشارقة، الإمارات

د. عبدالكريم صالح عبدالكريم
أستاذ القانون المدني المساعد
كلية القانون والعلوم السياسية
جامعة دهوك، العراق

الملخص

يُعدُّ عنوان برتوكول الإنترنت الـ «IP address» المُعرِّف الرقمي لأي جهاز مُتصل بشبكة الإنترنت، وبالتالي فإن ترجمة هذا المُعرف الرقمي، عبر الخبرة الرقمية التي تقوم بفك الشفرات المتعلقة بالعلاقة بين الرقمين «0» و«1»، والأرقام التعريفية لكل جهاز، سواء أكان جهاز حاسوب مكتبي أم جهاز حاسوب محمول (لاب توب) أم جهاز هاتف ذكي، أو أي جهاز يسمح باستعمال شبكة الإنترنت عبر الشبكة اللاسلكية «Wi Fi» أو بالربط السلكي؛ وعادة ما تقود معرفة هذا العنوان إلى معرفة شخص مالك الجهاز أو مستخدمه، وهذا ما قد يُعرِّض الحق في الخصوصية للانتهاك.

ولقد اتبعنا في هذا البحث الأسلوب التحليلي، حيث إن البحث في البعد القانوني لعنوان بروتوكول الإنترنت «IP address» له جوانب متعددة، تتصل الأولى منها بالمرحلة السابقة على محاولة كشف الخصوصية، والثانية متصلة بالمرحلة اللاحقة على كشف الخصوصية؛ أما المرحلة السابقة فتتعلق بمدى جواز إلزام الأشخاص بالكشف عن هوياتهم الشخصية عند اقتنائهم الأجهزة الإلكترونية، وهل يجوز لهم إخفاء هوياتهم عند استخدامهم لها؟ ومن الذي يحق له متابعة الأشخاص والكشف عن هوياتهم والإبلاغ عنهم، وهل يجوز استعمال الخبرة الحِرفية في تقصِّي الكشف عن الأصحاب الحقيقيين أو المستخدمين الفعليين للأجهزة، لاسيما أجهزة الهواتف المحمولة (الموبايل)؟ ومتى يكون متاحاً للأشخاص فعل ذلك؟

أما المرحلة اللاحقة للكشف عن عنوان بروتوكول الإنترنت «IP address» فتتعلَّق بها جوانب تتصل بالمساءلة القانونية، لاسيما على الأشخاص الذين يتعمدون إخفاء هوياتهم الشخصية لارتكاب جرائم إلكترونية أو للتحرش أو المزاح بين من لم يتآلف المزاح بينهم، وما مدى مسؤولية مُتتبع عناوين بروتوكول الإنترنت «IP address» للكشف عن أسرار الأشخاص وخصوصياتهم، وخرق حساباتهم الرقمية أو المالية؟ كل

هذه الأفعال والسلوكيات ترتبط أشد الارتباط بالمنظومة الحمائية لحقوق الأشخاص في صون خصوصياتهم ومنع الاعتداء عليها.

وتم تقسيم الدراسة إلى مبحثين يسبقهما مطلب تمهيدي لبيان ماهية عنوان بروتوكول الإنترنت، وقد تم تخصيص المبحث الأول لتحديد الأبعاد القانونية للمرحلة السابقة على كشف عنوان بروتوكول الإنترنت «IP address»، أما المبحث الثاني فخصص للأبعاد القانونية للمرحلة اللاحقة على الكشف عن العنوان، على أن تكون خاتمة البحث لوضع أهم الاستنتاجات والتوصيات بشأن الدراسة، حيث دعت إلى ضرورة صياغة نص في قانون خاص بحماية الحق في الخصوصية، يمنع مزودي خدمات الإنترنت أو الاتصال ومحركات البحث ومواقع التواصل الاجتماعي، من تخزين البيانات الشخصية الخاصة للمستخدم، والمتعلقة بالأسرة أو بالسجل الإجرامي القديم، أو السمعة المالية، من خلال ملفات الكوكيز وعناوين بروتوكول الإنترنت إلا لأغراض الأمن العام والمصلحة العامة.

كلمات دالة: عنوان بروتوكول الإنترنت، المسؤولية المدنية، الإنترنت، هوية المستخدم، حماية البيانات الخاصة.

المقدمة

لا شك في أن المختصين في شؤون القانون الخاص يدركون تماماً حجم البحوث القانونية التي تتطرق إلى المسؤولية بشأن الخصوصية وحماية البيانات الشخصية للأفراد، لكن ومع تنوع وسائل انتهاك الخصوصية وبخاصة على شبكة الإنترنت، فقد ظهرت وسيلة جديدة للاعتداء على البيانات الخاصة للأفراد بمجرد قيامهم بربط أجهزتهم الإلكترونية المخصصة للاتصال بشبكة الإنترنت من أجهزة الكمبيوتر والهواتف المحمولة وغيرها، دون أن يدركوا حجم المخاطر التي تحيط بهم، والمتمثلة بإمكانية كشف هوياتهم كمستخدمين للشبكة، وهذا ما يتم إما من قبل محركات البحث الخاصة على الإنترنت كجوجل Google، أو مواقع التواصل الاجتماعي كفيسبوك Facebook، أو من قبل مزودي خدمة الدخول لشبكة الإنترنت، وذلك من خلال ما يسمى بعنوان بروتوكول الإنترنت «IP address»، الذي يُعيّن لكل مستخدم مرتبط بالشبكة، وهو ما يساعد المواقع التي يزورها أو يستخدمها في الاقتفاء المكاني عنه، وكشف هويته بواسطة تخزين بياناته الشخصية.

وإزاء كثرة النزاعات والشكاوى التي تتعلق بانتهاك الخصوصية، اضطر الاتحاد الأوروبي إلى وضع قواعد جديدة بهذا الخصوص، تلزم الشركات التي لها محركات بحث أو مواقع تواصل اجتماعي بعدم تخزين المعلومات أو البيانات الشخصية لمستخدمي شبكة الإنترنت، إلا للغرض الذي أعد له عنوان برتوكول الإنترنت (IP) ولفترة معينة، أما بعد ذلك فإن تلك الجهات تكون مسؤولة عن كشف هوية المستخدم.

مشكلة البحث

تتعلق مشكلة البحث بوجود فراغ قانوني في التشريع الوطني فيما يتعلق بالحلول التشريعية لمواجهة قضايا انتهاك الخصوصية بشكل عام، خاصة أن القوانين التي تتعلق بالاتصالات لا تتصدى لفرضية عنوان برتوكول الإنترنت (IP)، وكيف يمكن أن تؤثر سلباً على الخصوصية والبيانات الشخصية للأفراد، وعلى هذا وفي إطار حماية حق الإنسان في الخصوصية، تأتي هذه الدراسة لبيان التكييف القانوني لعنوان بروتوكول الإنترنت (IP)، وكيفية تأثيره على الحياة الخاصة للأفراد والسبل اللازمة لمنع ذلك.

منهج البحث

سيتم بحث موضوع تأثير عنوان بروتوكول الإنترنت على الخصوصية، من خلال إجراء دراسة تحليلية لآراء الفقه والقوانين ذات الصلة، في ضوء الدراسة المقارنة مع

التنظيم العام لحماية البيانات الأوروبي GDPR 2016/679 والقوانين الأجنبية الأخرى، وذلك أينما اقتضت الحاجة.

خطة البحث

ولأجل الإحاطة بموضوع البحث، ارتأينا تقسيم البحث وفق الخطة الآتية:

البدء بمطلب تمهيدي ويخصص لبيان ماهية عنوان برتوكول الإنترنت (IP)، ثم يأتي المبحث الأول لتحديد الأبعاد القانونية للمرحلة السابقة على كشف عنوان برتوكول الإنترنت«IP address»، أما المبحث الثاني فيخصص للأبعاد القانونية للمرحلة اللاحقة على الكشف عن عنوان الـ «IP address»، على أن تكون خاتمة البحث لوضع أهم الاستنتاجات والتوصيات بشأن الدراسة.

مطلب تمهيدي

ماهية عنوان بروتوكول الإنترنت «IP address»

لعنوان برتوكول الإنترنت «IP address» مفهوم تقني وآخر قانوني، وله وظائف في مجال شبكات الإنترنت، ويمتاز بمجموعة من الخصائص كذلك، وله دور مُعيَّن في سبيل الكشف عن أجهزة الاتصال المربوطة بشبكة الإنترنت، والذي ينعكس سلباً على الخصوصية وحماية البيانات الخاصة.

وعليه سنتناول هذه المسائل بتقسيم هذا المطلب إلى فرعين.

الفرع الأول

تعريف عنوان بروتوكول الإنترنت «IP address» وتحديد وظائفه

يتم تعيين عنوان بروتوكول إنترنت لكل مشترك متصل بالشبكة، وهو العنوان الذي يسمح للمستخدم الاتصال بالأجهزة المتصلة بالشبكة، والكلام نفسه ينطبق على خدمات الاتصال المتنقلة التي توفر الاتصال بشبكة الإنترنت من خلال جهاز الهاتف الذكي.

ومن هنا فإن الاعتماد على عنوان برتوكول الإنترنت «IP address» قد يكون له انعكاساته على الخصوصية والبيانات الشخصية للمستخدم، فيمكن استخدام هذه العناوين لمعرفة كافة أنواع السلوك عبر الإنترنت، كمن يشارك في نشاط سياسي أو ديني على هذه الشبكة، وكذلك مسألة الوصول إلى المواد الإباحية، وانتهاك حقوق الملكية الفكرية.

وعلى هذا كثيراً ما نسمع أن شركة جوجل Google أو فيسبوك Facebook أو تويتر Twitter بأنها متهمة بقيامها بكشف البيانات الشخصية للعملاء إلى السلطات لأغراض معينة، سواء أكانت أمنية أم غيرها. ومن خلال دراسة لمكتب مفوضية الخصوصية في كندا تبيَّن أنه من خلال عنوان برتوكول الإنترنت «IP address»، تم التعرف على عدد مرات زيارة الشخص لمواقع معينة على الشبكة لأغراض تعود للمشورة القانونية واللياقة البدنية، وتبادل الصور، والبحث عن جماعات دينية محددة وغير ذلك[1].

(1) Stuart Hargreaves and Lockman Tsui, IP address as personal data under Hong Kong privacy law, an introduction to the access my info HK project, the Chinese university of Hong Kong faculty of law research paper no.2017-23, journal of information, law & science 25(2).

ويذهب البعض إلى أن معلومات التعريف الشخصية أو ما تسمى بالبيانات الشخصية – والتي يعد عنوان برتوكول الإنترنت «IP» من بينها – هي أي بيانات تستخدم لتحديد هوية شخص ما أو الاتصال به أو تحديد موقعه، وهي معلومات معيّنة، كالاسم ورقم الضمان الاجتماعي ورقم الهاتف والعنوان البريدي كمعلومات شخصية.

ويُعرَّف عنوان بروتوكول الإنترنت بأنه: «سلسلة من الأرقام التي تحدد جهاز الكمبيوتر أو الطابعة أو الهاتف أو أي جهاز آخر متصل بالإنترنت»[2]. وعُرّف أيضاً بأنه: تسمية رقمية فريدة لجهاز على الإنترنت. ويتم التعرف على كل جهاز من خلال عنوان بروتوكول الإنترنت «IP» وتمكين الوصول إلى الإنترنت، مثال ذلك عنوان IP:51.254.100.34، ويمكن أن يكون عنوان بروتوكول الإنترنت «IP» ثابتًا أو ديناميكيًا.

وقد تم تعريفه كذلك بأنه: «سلسلة من أربعة أرقام بين (0 و255) تستخدم لتحديد جهاز الكمبيوتر المتصل بالإنترنت[3]. وعنوان بروتوكول الإنترنت «IP» الديناميكي هو فئة متغيرة، مما يعني أنه كلما تمت إعادة تعيين جهاز توجيه متصل بالإنترنت، يأخذ عنوان بروتوكول الإنترنت «IP» قيمة مختلفة.

كقاعدة عامة، يقوم مزود خدمة الإنترنت بتعيين عنوان بروتوكول إنترنت «IP» ديناميكي للمستخدم، ما لم يطلب المستخدم خلاف ذلك، ويكفي هذا لتصفح الإنترنت بانتظام. ومع ذلك، إذا كانت متطلبات المستخدم أكبر، وإذا كان الوصول المستمر إلى بعض المواد عبر الإنترنت ضروريًا (على سبيل المثال تثبيت المراقبة بالفيديو عبر الإنترنت)، فسيختار المستخدم عنوان برتوكول إنترنت «IP» ثابتًا.

وتم تعريف عناوين برتوكول الإنترنت «IP» كذلك بأنها معرَّفات تبدو كسلسلة من الأرقام المفصولة بينها بالنقاط مثل 122.41.123.4، بحيث إنه في كل مرة يريد المستخدم الوصول إلى الإنترنت، فسينسب إليه عنوان بروتوكول إنترنت «IP» خاص بالجهاز الذي يستخدمه للوصول إلى الشبكة[4].

(2) Frederick Lah, Are IP address personally identifiable information?, Journal of law and policy for information society, vol.4:3, 2008, p.682.

(3) AJ Pénal n° 3/2009 de mars 2009, «Dossier Cybercriminalité: morceaux choisis», p. 120. 26; O. Itéanu «L'identité numérique», p.16.
د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية عبر شبكات التواصل الاجتماعي، ص1943. بحث متاح على الرابط الإلكتروني:
https://mksq.journals.ekb.eg/article_30623_1ab2f80af612aa4568dbf6239b535ac2.pdf.

(4) Eneken Tikk, IP addresses subject to personal data regulation, Paper available at: https://ccdcoe.org, Last accessed on: 5-12-2019.

أما بحسب المبادئ الدولية والضرورية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات لسنة 2014، فإن عناوين بروتوكول الإنترنت «IP» تُعرَّف بأنها: «بيانات الاقتفاء المكاني لمستخدم الأجهزة الإلكترونية المتصلة بشبكة الإنترنت»[5].

ويوجد نوعان من عنوان بروتوكول الإنترنت «IP address» وهما: العنوان الخاص والعنوان العام؛ أما العنوان الخاص، فهو يستخدم للاتصال داخل الشبكة نفسها باستخدام بيانات بروتوكول الإنترنت «IP» الخاصة، أو المعلومات التي يمكن إرسالها واستقبالها داخل الشبكة نفسها، وأما العنوان العام، فهو الذي يجهز بواسطة مزود خدمة الإنترنت «ISP» للاتصال خارج الشبكة.

وفي قرار حديث صادر عن محكمة العدل الأوروبية، وذلك في قضية Patrick Breyer v Bundesrepublik Deutschland[6]، والتي تتعلق بمدى أحقية السلطات الألمانية بالاحتفاظ بعناوين بروتوكول الإنترنت لأفراد عند زيارتهم لبعض المواقع الإلكترونية الحكومية، كتلك التي تتعلق بوكالة الأمن القومي حتى تتمكن من منع الهجمات الإلكترونية وكشفها، فقد تم تكييف عنوان بروتكول الإنترنت على أنه من قبيل المعلومات الشخصية[7].

وتتلخص وقائع القضية في أن (برايرِ) الألماني الجنسية، وهو عضو في أحد الأحزاب السياسية المعارضة، حينما عرف بأن بعض المواقع الحكومية تقوم بتخزين وتسجيل عناوين بروتوكول الإنترنت «IP» الخاصة بالزائرين، قام برفع دعوى على الحكومة الألمانية مدعياً أنه بتسجيل عنوان بروتوكول الإنترنت «IP» الخاص به، كانت الحكومة تعالج بياناته الشخصية بشكل غير قانوني. وجادل المدعي بأن هذه العناوين ينبغي اعتبارها بيانات شخصية.

---

(5) المبادئ الدولية والضرورية Necessary and proportionate لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات، النسخة النهائية، آيار/ مايو، 2014، ص6.

(6) Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland.

(7) وعلى خلاف ذلك، ذهب مفوض الخصوصية في هونغ كونغ إلى أن عنوان بروتوكول الإنترنت ليس ببيانات شخصية، لأنها تخص جهاز كمبيوتر وليس فرداً، وذلك بخصوص شكوى رفعت ضد شركة ياهو Yahoo تتهمها بالقيام بالإفصاح عن بعض البيانات التي تتعلق بصحافي إلى السلطات الصينية، وذلك بتاريخ 2017/3/15، حيث كتب المفوض في تقريره بأن هذه العناوين في حد ذاتها لا تكفي لكي تكون بيانات شخصية. وللرد على ذلك نقول: إن هذه البيانات إذا ما ادمجت مع معلومات أخرى، فإنها تعد بيانات شخصية. انظر:

Pinsent Masons, Out-Law-Guide, IP addresses and the Data Protection Act, available at: https://www.pinsentmasons.com/out-law/guides/ip-addresses-and-the-data-protection-act, Last accessed on: 12-3-2020.

وبعد رفع القضية إلى محكمة العدل الأوروبية اعتبرت هذه المحكمة أن المعلومات هي بيانات شخصية، طالما كان بإمكانها تحديد هوية الشخص بشكل مباشر أو غير مباشر، ووفقاً لذلك من الممكن أن يتم الاحتفاظ بتلك البيانات من قبل شخص ثالث وليس مجرد مزود خدمة الإنترنت.

وانتهت المحكمة إلى أن تلك العناوين والتي يحتفظ بها مشغل موقع الويب هي من قبيل المعلومات الشخصية، طالما أن المشغل لديه الوسائل القانونية التي تمكنه من تحديد موضوع البيانات ببيانات إضافية لدى مزود خدمة الإنترنت حول هذا الشخص، ما لم يوجد حظر قانوني أو أي حظر آخر على مشاركة مزود خدمة الإنترنت لبيانات المشترك[8].

وفيما يتعلق بوظائف عنوان بروتوكول الإنترنت «IP»، فإنه يمكن الإشارة إلى ما يلي:

1- يعد وسيلة لتحديد هوية مستخدم شبكة الإنترنت ومعرفة المواقع الإلكترونية التي قام بزيارتها.

2- تحديد الجهة التي يستخدم فيها الشخص شبكة الإنترنت، بعبارة أخرى فإن التصفح على شبكة الإنترنت يترك مجموعة من المعلومات من بينها إمكانية حفظ عنوان بروتوكول الإنترنت «IP»، والذي يمكن من خلاله تحديد اسم النطاق، وتبعاً له اسم الشركة أو الجهة التي قامت بتسجيل النطاق[9].

3- تحديد الكلمات التي قام المستخدم بالبحث عنها في محركات البحث، والحوارات التي أجراها وتبادل الرسائل الإلكترونية[10]. وفي كل مرة يقوم فيها المستخدم باستخدام محركات البحث، فإن الموقع يسجل تلقائياً معلومات المستخدم في سجل الخادم، مع تحديد الجهة التي زار منها الموقع، وتعيين عنوان بروتوكول الإنترنت «IP» الخاص به.

4- إن عنوان بروتوكول الإنترنت يمكن أن يؤدي مجموعة من الوظائف، من بينها أن جميع مواقع الويب تحتاج إلى معلومات بروتوكول الإنترنت «IP» لمعرفة مكان نقل البيانات، كما أن محركات البحث تحتاج إلى مثل هذه المعلومات لضبط عمليات الاحتيال خاصة فيما يتعلق بمسائل الإعلانات التجارية، كما أن تلك

(8) Daniel Felz, ECJ Declares IP Addresses are Personal Data, October 19, 2016.

(9) مصطفى عائشة بن قارة، الحق في الخصوصية المعلوماتية بين التحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، غزة، فلسطين، المجلد الثاني، العدد 5، 2016، ص42.

(10) د. منى تركي الموسوي و جان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013، ص13.

المعلومات الخاصة بعنوان بروتوكول الإنترنت «IP» تستخدم لتحسين جودة عمليات البحث، وأخيراً تستخدم تلك المعلومات لمعرفة أماكن في الشبكات يكون فيها تأخير عند الاستجابة للطلبات[11].

الفرع الثاني

خصائص عنوان بروتوكول الإنترنت «IP address» ودوره في كشف الخصوصية

لعنوان بروتوكول الإنترنت عدة خصائص من ضمنها:

1. يكون عنوان بروتوكول الإنترنت «IP» منفرداً، أي لا يجوز أن يكون لجهازي كمبيوتر عنوان بروتوكول الإنترنت «IP» نفسه في الشبكة نفسها، وإن حصل هذا فإن خللاً سيحدث في الشبكة.
2. يتكون عنوان بروتوكول الإنترنت «IP» من 32 بت، ويقسم إلى أربع خانات 192.168.12.5.
3. عادة يتم اختراق أجهزة الحاسوب عن طريق معرفة عنوان بروتوكول الإنترنت.
4. يختلف عنوان بروتوكول الإنترنت «IP» في الشبكات الداخلية غير المغلقة Compra windows عن عنوان بروتوكول الإنترنت «IP»، بمعنى أن الشبكة الداخلية لها عدد مفتوح، وعنوان بروتوكول الإنترنت «IP» الداخلي وغير مدفوع الثمن غير عنوان بروتوكول الإنترنت «IP» الحقيقي، فهو يتعامل مع الإنترنت، ويرسل البيانات ويستقبل أيضاً، ومدفوع الثمن.
5. هناك شركات كاملة تعمل لخدمات توزيع الإنترنت وبيع عنوان بروتوكول الإنترنت «IP» الحقيقي للعملاء والشركات[12].

وعن قابلية عنوان بروتوكول الإنترنت «IP» في كشف خصوصية المستخدمين[13]، فإنه

(11) Frederick Lah, Op. Cit., p. 693.

(12) مقال بعنوان «عنوان الـ آي بي»، متاح على الموقع الإلكتروني: https://www.marefa.org، تاريخ الدخول للموقع في: 2020/2/4.

(13) نقصد بالخصوصية محل الدراسة الخصوصية المعلوماتية، وهي التي تتمثل بالقواعد المنظمة لجميع إدارات البيانات الخاصة الموجودة على الأجهزة الإلكترونية أو على شبكة الإنترنت، فهي حق الأفراد في أن يحددوا لأنفسهم متى وكيف وأين يمكن للمعلومات الخاصة أن تصل للآخرين، وحفظها وتسجيلها ومعالجتها رقمياً. انظر: د. هانيا فقيه دندش، دراسات في القانون الخاص، 5- حماية الحق في الخصوصية المعلوماتية، الجزء الأول، ط1، منشورات زين الحقوقية، بيروت، 2019، ص120 وما بعدها.

وفقاً للمشرف العام على حماية البيانات في الاتحاد الأوروبي بيتر هوستينكس يتعين على الشركات ومحركات البحث ومواقع التواصل الاجتماعي أن تتعامل مع سجلات عناوين بروتوكول الإنترنت «IP» على أنها بيانات شخصية، ولا يلزم للشركة أن تقوم بمعالجة البيانات الشخصية لمعرفة بعض التفاصيل كالاسم وتاريخ الميلاد، أو أية بيانات أخرى شخصية للشخص الذي كان يُراقب نشاطه(14).

وهذا كان موقف التوجيه الأوروبي الخاص بحماية البيانات EC/46/1995، وكذلك التوجيه الأوروبي الخاص بالخصوصية والاتصالات الإلكترونية EC/58/2002. أما عن موقف القانون العراقي من هذه المسألة، فعلى الرغم من عدم وجود قانون خاص بحماية الحق في الخصوصية بشكل عام، وانتهاك هذا الحق من خلال عنوان بروتوكول الإنترنت بشكل خاص، إلا أنه بالرجوع إلى الدستور العراقي لسنة 2005 نجده ينص في المادة (17) على أنه: «لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والآداب العامة»، لكن هذا النص وإن كان يتعلق بحماية الحق في الخصوصية، إلا أنه نص عام، وكان ينبغي فيه الإشارة إلى حماية هذا الحق في البيئة الإلكترونية، بعكس الدستور المصري المعدَّل في عام 2019، حيث جاء في المادة (57) منه أن: «للحياة الخاصة حرمة، وهي مصونة، لا تمس، وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة وسريتها مكفولة، ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة، وفي الأحوال التي يبينها القانون...».

ويمكن القول إن النص الوارد في هذه المادة جاء دقيقاً للغاية، وبموجبه فإن أية بيانات شخصية تقدم أثناء الاتصالات والمراسلات التي يقوم بها المستخدم ينبغي فيها أن تكون سرية، ولا يجوز لمقدمي خدمة الاتصال بالإنترنت أو حتى محركات البحث على الشبكة ومواقع التواصل الاجتماعي الاحتفاظ بها إلا لغاية معينة ولمدة محددة. في حين نجد أن المشرع الفرنسي قد نص في الفقرة الأولى من المادة الثانية من التقنين المدني لسنة 1804(15) على أنه: «لكل شخص الحق في أن تحترم حياته الخاصة». ومن هذا النص يُلاحظ أن المشرع الفرنسي قدم حماية عامة للحياة الخاصة.

(14) Eneken Tikk, Op. Cit., p. 30.

وأكد المشرف في الإتحاد الأوروبي أن: «مبادئ الحماية ينبغي أن تطبق على أي شخص معرف أو قابل للتحديد، فمثلاً لو أراد المستخدم تحميل مادة ما على شبكة الإنترنت، فقد يتم تعريف المستخدم والكشف عن هويته من قبل أطراف ثالثة من خلال عنوان بروتوكول الإنترنت «IP» الذي استخدمه لذلك، ولهذا فلا يجوز جمع وتخزين تلك العناوين إلا لأسباب تتعلق بالاتصال نفسه، بما في ذلك الفواتير ومنع الاحتيال. أما بعد ذلك، فيجب محو تلك البيانات، دون المساس بالحق الخاص بالسلطات في جمع البيانات للشرطة والمدعين العامين للتحقيق في جريمة خطيرة».

(15) تم تعديل التقنين المدني الفرنسي بموجب الأمر التشريعي رقم 131 لسنة 2016.

وكانت الوكالة المعنية بحماية البيانات في فرنسا قد غرمت شركة جوجل (Google) 50 مليون يورو بداية عام 2019 لانتهاكها قواعد الاتحاد الأوروبي للخصوصية على الإنترنت، وبحسب المحكمة فإن محرك البحث الخاص بالشركة يفتقر إلى الشفافية والوضوح في الطريقة التي يبلغ بها مستخدميه بتعامله مع البيانات الشخصية، ويتم ذلك بشكل خاص من خلال خرائط جوجل Google maps[16].

وفي سنة 2008 قام الاتحاد الأوروبي بتشكيل لجنة استشارية للعمل على المادة (29) من التوجيه الأوروبي الخاص بحماية البيانات، لتكييف حقيقة عناوين بروتوكول الإنترنت «IP»، ولقد خلصت في تقريرها إلى أن هذه العناوين وملفات تعريف الارتباط كوكيز Cookies، التي تحتوي على معرّف فريد هي بيانات شخصية.

وأكدت اللجنة أنه ينبغي على محركات البحث – والتي هي معالجة للمعلومات – ومواقع الويب بشكل عام الالتزام بأن المعلومات الخاصة بعناوين بروتوكول الإنترنت ستعالج بطريقة قانونية وعادلة، والتأكد من أن البيانات تُجمع فقط لأغراض معينة وصريحة. كما يتعين أن تكون معالجة تلك البيانات لمرة واحدة وعلى صلة بالغرض الذي من أجله تم خزنها وجمعها.

وذكرت اللجنة أن الاحتفاظ بعناوين بروتوكول الإنترنت «IP» يجب أن يكون لفترة تقل عن ستة أشهر من أجل تحسين الشفافية، وضمان المعالجة العادلة والتناسب مع الغرض الذي يبرر هذا الاستبقاء، وإذا احتفظ مقدمو خدمة البيانات بهذه العناوين لفترة أطول، فقد خلصت الفرقة الاستشارية إلى أنه على مقدمي الخدمة أن يثبتوا بشكل واضح حاجتهم إلى أن ذلك ضروري للخدمة. وأوضحت اللجنة أنه بمجرد أنه لم يعد هناك غرض مشروع لاستخدام البيانات، فعلى مقدمي الخدمات حذف تلك العناوين والمعلومات، أو جعلها مجهولة المصدر[17].

(16) رنا أبتر، خرائط غوغل تتبعك أينما كنت، صحيفة الشرق الأوسط، 19 كانون الأول/ ديسمبر 2019، العدد 14996.

(17) Frederick Lah, Op. Cit., p.696; also: Article (17) of general data protection of EU. Which mentioned that: (Right to be forgotten):

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
   a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   b) the data subject withdraws consent on which the processing is based according

ومن نتائج تقرير اللجنة العاملة في هذا المجال كذلك التوصية بعدم الاستخدام المفرط لعناوين بروتوكول الإنترنت «IP» الخاصة بالمستخدمين، بل أوجبت استخدامها فقط للغرض الذي من أجله تم تخزينها. ويمكن تشبيه هذا القول بالتعسف في استعمال الحق المنصوص عليه في القانون المدني، ذلك لأنه وإن كان من حق محركات البحث ومزودي خدمة الإنترنت الاحتفاظ بالمعلومات من خلال عنوان بروتوكول الإنترنت «IP»، غير أنها تكون متعسفة حينما تحتفظ بها أكثر من اللازم، ولغرض غير الذي أعد من أجله هذا العنوان.

وتجدر الإشارة إلى أن محكمة استئناف باريس قد ذكرت في قرارين منفصلين أن

to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;

b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e) for the establishment, exercise or defence of legal claims.

معلومات عناوين بروتوكول الإنترنت «IP» لا يمكن أن تعد معالجة لبيانات شخصية، وذلك لأن أرقام التعريف تتعلق بالجهاز وليس الشخص الذي يقف وراء الآلة أو الجهاز الإلكتروني[18]، لكن المشرف العام على حماية البيانات في الاتحاد الأوروبي (الذي أشرنا إلى اسمه سابقاً) وقف ضد هذا الاتجاه – وهذا ما نؤيده في بحثنا – وذهب إلى أنه لكي يتم احتساب عناوين بروتوكول الإنترنت «IP» كبيانات شخصية، فليس بشرط أن تعرف الشركة المعالجة اسم الشخص الذي كانت تراقب نشاطه، فيمكن تحديد هوية الشخص من خلال بياناته الشخصية، فالبيانات من دون اسم يمكن أن تظل شخصية[19].

(18) Meryem Marzouki, Is the IP Address Still a Personal Data in France? European Digital Rights, Sept. 12, 2007, http://www.edri.org/edrigram/number5.17/ip-personal-data-fr. last visiting: Februray18, 2020.

(19) Hustinx: Nameless Data Can Still be Personal, Out-Law.Com, Nov. 6, 2008, http://www.out-law.com/page-9563, Last accessed on: 18-02-2020.

المبحث الأول
الأبعاد القانونية للمرحلة السابقة على كشف عنوان بروتوكول الإنترنت «IP address»

يشتمل هذا المبحث على مطلبين: يخصص أولهما للحديث عن اقتناء الأجهزة الإلكترونية ومدى الإلزام بكشف الهوية، أما المبحث الثاني فسيكون لأبعاد الخصوصية في استخدام الأجهزة الإلكترونية.

المطلب الأول
اقتناء الأجهزة الإلكترونية ومدى الإلزام بكشف الهوية

في هذا المطلب سنتطرق لمسألتين هما الوسائل التي يمكن من خلالها للشخص أو لجهة معينة الحصول على جهاز إلكتروني يستخدم في الاتصال مع شبكة الإنترنت، أما المسألة الثانية فهي مدى إمكانية إلزام الشخص بكشف هويته.

الفرع الأول
وسائل اقتناء الأجهزة الإلكترونية والكشف عن الهوية

إن الشائع الآن هو أن الأجهزة المتصلة بالإنترنت والتي تدخل في إطار خصوصية الأفراد هي إما أجهزة الاتصال اللاسلكي، ونقصد بها تحديداً الهاتف المحمول، والكمبيوتر وأجهزة المودم الخاصة بخدمة الإنترنت كجهاز الفاست لينك Fast link ونيوروز Newroz وغيرها، وأخيراً كاميرات المراقبة بمختلف أشكالها.

والسؤال هنا ما هي الوسائل التي يمكن من خلالها اقتناء تلك الأجهزة؟ في الحقيقة لا تتعدى المسألة في كون الوسيلة تكمن في إبرام عقد لشرائها، وذلك من المحلات التي تزاول هذه المهنة، وهي شركات أو بائعو تجزئة، أو أن الشخص بإمكانه الحصول على جهاز إلكتروني من خلال الاشتراك بخدمة الاتصال مع شركة اتصال معينة، أو أن الشخص يقتني ذلك الجهاز بحكم عمله لدى جهة معينة حكومية أو غير حكومية.

واقعياً، نرى أن الشركات – التي تقوم بالتجارة في مجال أجهزة الهواتف المحمولة من خلال عقود الاشتراك الرسمية – تقوم بتسجيل بيانات المشترك لديها، تتضمن اسمه ولقبه وتاريخ ميلاده ورقم هاتفه، بل تحتفظ بنسخة مصورة وملونة من هوية الأحوال

المدنية للشخص المشترك. والكلام نفسه ينطبق على مزودي خدمة الإنترنت «ISP» Internet Service Provider .

وتكمن المشكلة في أن أجهزة الهواتف المحمولة تلك قد تكون بيد شخص حائز وليس المشترك نفسه، حيث تجد أن هناك الكثير من شرائح الهواتف المحمولة (Sim Card) تباع في محلات دون أن يطلب البائع أية بيانات تتعلق بالمشتري، وفي هذا نصت المادة (6) من قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان– العراق رقم 6 لسنة 2008 على أنه: «على شركات الاتصالات العاملة في الإقليم اتخاذ ما يلي: أولاً– تسجيل بطاقة الموبايل الإلكترونية وأجهزة الاتصالات الإلكترونية والهواتف النقالة الأخرى الصادرة منها قبل نفاذ هذا القانون باسم الحائز غير المشترك، وذلك خلال مدة ستة أشهر من تاريخ نفاذه وإلغاء بطاقة الحائز الذي يتخلف عن مراجعة الشركة خلال تلك المدة. ثانياً– تقديم أية معلومة متعلقة ببطاقة الاشتراك والمشترك إلى المحكمة المختصة عند الاقتضاء. ثالثاً– تعاقب الشركة المخالفة للفقرتين (أولاً وثانياً) من هذه المادة بغرامة لا تقل عن خمسين مليون دينار، ولا تزيد على مائة مليون دينار».

وبالنسبة للقانون الفرنسي، فقد فرض المشرع التزاماً على من يقوم بالمعالجة الإلكترونية للبيانات الشخصية، وذلك بالكشف عن كل ما يقوم به من إجراءات تتعلق بالبيانات الشخصية منذ تجميعها، وكذلك الالتزام بعدم إفشاء البيانات الشخصية للغير، إذا كان إفشاء هذه البيانات من شأنه أن يهدد اعتبار من تخصه هذه البيانات أو حياته الخاصة[20].

وعلى هذا يلتزم مزود خدمة الإنترنت باتخاذ تدابير فعَّالة لحماية معلومات العميل من الاستخدام غير المصرح به لتلك المعلومات، أو الكشف عنها أو الوصول إليها، كما يلتزم مزود خدمة الإنترنت بإخطار المستهلك باختراق بياناته بأسرع وقت. وبخلاف ذلك يتحمل مزود الخدمة المسؤولية المدنية (العقدية) الناجمة عن الضرر الذي يلحق بالمستهلك، والمتمثل في كشف هويته وبياناته الشخصية من قبل الغير، والمسؤولية تكون بناءً على وجود خطأ مشترك بين الغير والمزود[21].

(20) د. سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، مجلة دراسات قانونية وسياسية، جامعة السليمانية، العراق، السنة السادسة، العدد 11 نيسان/أبريل 2018، ص195.

(21) The EU working party Working Document, Privacy on the Internet - An integrated EU Approach to On-line Data Protection, Adopted on 21st November 2000, p.18. Available at: ec.europa.eu. last visiting: May 13, 2020.

وفي الحقيقة، فإن التزام مزود خدمة الاتصال بصفة عامة وخدمة الإنترنت تحديداً، يعد التزاماً بالامتناع عن القيام بعمل، وهو الامتناع عن كشف الخصوصية للمشترك، ويعد تنفيذ هذا الالتزام من مقتضيات حسن النية، حيث جاء في المادة (150) من القانون المدني العراقي بأنه: «يجب على المتعاقدين تنفيذ التزاماتهما بحسن نية». كما جاء فيه أنه: «لا يقتصر العقد على ما ورد فيه، بل يشمل ما هو من مستلزماته وفق القانون والعرف والعدالة وبحسب طبيعة الالتزام». وعلى هذا يلتزم مورد الخدمة بالامتناع عن كشف خصوصية المستخدم وإن لم ينص على ذلك في العقد.

الفرع الثاني

تداول الأجهزة الإلكترونية ومدى الالتزام بكشف الهوية

أما بالنسبة للتساؤل الآخر والذي طرحناه في مقدمة البحث، فيتعلق بمدى الالتزام الواجب على مستخدمي أو مقتيني أجهزة الاتصال بالكشف عن هوياتهم عند اقتناء تلك الأجهزة، فيلاحظ أن للشخص الحق في الحياة الخاصة أو ما يسمى بالحق في الخصوصية، وهذا حق كفلته الدساتير ومن بينها دستور العراق لسنة 2005، حيث نصت الفقرة أولاً من المادة (17) منه على أنه: «لكل فرد الحق في الخصوصية الشخصية، بما لا يتنافى مع حقوق الآخرين، والآداب العامة».

إن المبدأ العام هو أنه يجب أن يكون لدى المستخدمين خيار الوصول إلى الإنترنت من دون الاضطرار إلى الكشف عن هوياتهم، حيث لا تكون البيانات الشخصية ضرورية لتوفير خدمة معينة، وعلى مزودي خدمة الإنترنت ومنتجي أجهزة الاتصال اتخاذ التدابير اللازمة لإخفاء هوية المستخدم[22].

وعلى هذا يكون من حق الفرد مقتني الجهاز الإلكتروني الحفاظ على أسراره أو بياناته الشخصية، ويمنع الغير من الوصول إليها، لكن نظراً لكثرة انتهاكات حقوق الغير في السمعة والصورة والخصوصية المعلوماتية وذلك من خلال الأجهزة الإلكترونية، يجد الفرد المراد حماية خصوصيته ملزماً بالكشف عن هويته لجهة معينة، وهذه الجهة قد تكون شركة اتصالات حكومية أو حتى غير حكومية، وذلك لمقتضيات المصلحة العامة المتمثلة في حماية الأمن والنظام العام[23]. فتجد المشترك في خدمة شبكة الإنترنت عاجزاً

(22) Op. Cit., p. 12.

(23) جاء في الأسباب الموجبة لقانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان أنه: «بالنظر للتطورات الاجتماعية والاقتصادية والسياسية التي طرأت على حياة المواطنين في إقليم كوردستان، وبالنظر لتطلع شبابه إلى التطورات التكنولوجية في العالم، وما ترافق هذه التطورات من

عن الانتفاع بهذه الخدمة ما لم يدل ببعض بياناته الشخصية لمزود تلك الخدمة، وكذلك الحال بالنسبة للاشتراك في خدمة الهواتف المحمولة.

لكن بالمقابل هناك تقنية تسمى في بي ان VPN، وهي تسمح لمستخدم الإنترنت بإخفاء هويته وبياناته عند الاتصال بشبكة الإنترنت في مواجهة مجرمي هذه الشبكة والهاكرز، فالمعروف أن مزود خدمة الإنترنت «ISP» تمر عليه جميع البيانات الخاصة بالمستخدمين المتصلين بالإنترنت عن طريقه، وعنده جميع السجلات الخاصة بالمواقع التي يتصفحها المستخدمون، وهو قادر على اعتراض جميع البيانات التي تنتقل إلى الإنترنت عن طريقه ومشاهدة محتواها، وقد يحتفظ بها لمدة معينة، والمشكلة هنا أن المستخدمين لا يعلمون ماذا سيفعل مزود خدمة الإنترنت بسجلاتهم وبياناتهم، فمن الممكن مثلاً أن يتعاون مع الحكومة عندما تطلب منه بيانات أحد المستخدمين، ولذلك وحفاظاً على الخصوصية، فإن أغلب المستخدمين يقومون بتشفير بياناتهم واتصالهم لتفادي مراقبة مزودي خدمة الإنترنت.

وخدمة في بي ان VPN تقوم – كما ذكرنا سابقاً – بتشفير اتصال المستخدم وبياناته، بحيث لا يستطيع مزود الخدمة الاطلاع عليها. وفي الدول التي تحد من حرية التعبير عن الرأي، قد يكون من الضروري على المستخدم إخفاء هويته تجنباً للملاحقة، وفي الواقع فإن مزود الخدمة ليس فقط قادراً على تحديد هوية صاحب أي عنوان بروتوكول الإنترنت IP Address، بل هو أيضاً يستطيع الكشف عن موقعه وغيرها من المعلومات عنه، وكل موقع تزوره باستخدام هذا العنوان يتم تسجيله من قبل صاحب الموقع، ومزود خدمة الإنترنت، وقد يتم تخزين هذه المعلومات لسنوات، ومن هنا فإن خدمة الـ VPN تمنح المستخدم عنوان بروتوكول إنترنت «IP» مجهولاً، يخفي العنوان الحقيقي، وهذا يجعل من المستحيل على محركات البحث أو مزود خدمة الإنترنت، أو حتى الموقع الذي يزوره المستخدم معرفة عنوان بروتوكول الإنترنت «IP» الحقيقي للمستخدم، مما يمنحه فرصة إخفاء هويته[24].

سهولة الاتصالات بين الشعوب، وحيث إن الهواتف الخلوية والبريد الإلكتروني ووسائل الاتصالات الحديثة هي ضرب من ضروب تلك التطورات، وما تحمل تلك الوسائل من أمور قد تؤثر سلباً على سلوك الشباب والأفراد والأطفال، وانطلاقاً من نهج حكومة إقليم كوردستان في إقامة مجتمع مدني متحضر على أسس سليمة، وبغية معاقبة من يسيء استعمال تلك الأجهزة، ومنعهم من التأثير على حريات الأفراد، وإفشاء أسرارهم الشخصية، والإساءة إلى الأخلاق والنظام العام والآداب العامة، لذا فقد شرع هذا القانون».

(24) مقال منشور في موقع http:/bahrainwatch.org بعنوان: «مميزات استخدام خدمة VPN»، تاريخ زيارة الموقع، 2019/12/21.

لكن السؤال الذي يثار هنا: هل من الجائز قانوناً استخدام تلك الخدمة، وقيام المستخدم بإخفاء هويته عند اتصاله بشبكة الإنترنت، وتداول الأجهزة الإلكترونية المتصلة بها؟ بعبارة أخرى هل استخدام خدمة الـ VPN قانوني؟

في الحقيقة، إن لكل دولة موقفها الخاص من تنظيم هذه الخدمة، فبعض الدول تحظر استخدام هذه الخدمة تماماً، ومن بينها العراق والصين وكوريا الشمالية والإمارات العربية المتحدة على سبيل المثال، وبعض الدول تسمح باستخدامها كالولايات المتحدة الأمريكية[25]، ومع ذلك فحتى بالنسبة للدول التي تسمح باستخدام تقنية إخفاء عنوان بروتوكول الإنترنت «IP»، فإن ذلك يعد فعلاً غير قانوني إذا استخدم لارتكاب فعل غير مشروع، مثل تنزيل المعلومات المحمية بموجب قوانين الملكية الفكرية، والتسلل إلى الأجهزة الإلكترونية دون ترخيص، والتحايل على التدابير التكنولوجية لمواقع الويب والتطبيقات[26]. وعلى أي حال، يمكن القول إن استخدام تلك التقنية بدافع حماية الخصوصية بحسن نية يكون جائزاً.

المطلب الثاني

الخصوصية في استخدام الأجهزة الإلكترونية

لا نزاع في أن المستخدم لشبكة الإنترنت والأجهزة الإلكترونية المتصلة بها له حق في حماية خصوصيته من شتى الوسائل التي تهددها، ومن بينها تتبع عنوان بروتوكول الإنترنت «IP» الخاص به، وذلك بعدم استعمال البيانات الشخصية المرتبطة به إلا حيث يوافق على ذلك هو نفسه، لكن ذلك مرهون بحسن استخدامه لتلك الأجهزة، بمعنى لو

(25) من القضايا المشهورة بشأن مشروعية إخفاء المستخدم لهويته وعدم الكشف عنها، القضية المعروفة باسم Krinsky v. Doe 6، عام 2008، حيث تتلخص وقائعها بقيام رئيس شركة برفع دعوى على عشرة من المدعى عليهم مع استدعاء موقع ياهو في كاليفورنيا بالإخبار عن هوياتهم، إلا أن أحدهم والذي يسمى Doe6 رفض ذلك، وطالب بإلغاء موضوع الكشف لأن من شأن ذلك التعارض مع حقه في (الغفلية) بموجب الدستور الأمريكي المعدل، وهذا ما أكدته محكمة استئناف كاليفورنيا بعد نقضها حكم المحكمة الابتدائية. انظر: أروى تقوى، الغفلية على الإنترنت بين سندان الحق في الخصوصية ومطرقة المسؤولية، مجلة المنارة للبحوث والدراسات، جامعة آل البيت، الأردن، المجلد 20، العدد 1، 2014، ص272.

(26) KIM porter, Are VPNs legal or illegal? Paper available at: https://us.norton.com/internetsecurity-privacy-are-vpns-legal.html, Last accessed on: 22/2/2020.
ولاحظ كذلك: د. عبد الكريم صالح عبد الكريم، تدابير الحماية التكنولوجية ودورها في حماية المصنفات الرقمية: دراسة تحليلية مقارنة، مجلة الحق، جمعية الإمارات للمحامين والقانونيين، العدد 17، سنة 2013، ص103–154.

أن المستخدم أساء استعمال الجهاز الإلكتروني وشبكة الإنترنت كأن يرتكب من خلالهما جريمة إلكترونية، فسيكون عرضة بلا شك لضرورة مراقبته من قبل الأجهزة المختصة، وتقتضي هذه المراقبة الكشف عن هويته من خلال ذلك العنوان، مما يشكل انتهاكاً للخصوصية، أما في غير ذلك فتتبع العنوان الخاص بالمستخدم من قبل أية جهة يكون اعتداءً على حقه في الخصوصية التي تستوجب المسؤولية.

الفرع الأول

أبعاد الخصوصية في استخدام الأجهزة الإلكترونية

إن مرتكز الخصوصية في استخدام الأجهزة الإلكترونية هو المحافظة على السرية، ومنع التدخل في شؤون الفرد، من خلال حماية بياناته الشخصية، بشكل يمنع انتشار المعلومات، وإيصالها إلى الآخرين، أو مراقبة ورصد تحركات المستخدم للجهاز الإلكتروني[27].

وتتمثل الجوانب القانونية، للاعتداء على الخصوصية، باستخدام البيانات الشخصية، بطريقة غير قانونية، في عدد من الجرائم، والأعمال غير القانونية، التي يمارسها الأفراد، أو الجهات الحكومية، ومنها: التنصت، والابتزاز، واختراق أنظمة المعلومات، والوصول إلى الأسرار المهنية والتجارية، إضافة إلى الرصد غير المشروع لحركة الأشخاص والأموال، من قبل الأجهزة الحكومية، وتكوين ملفات معلومات، دون سبب قانوني، والتمييز العنصري، والعقائدي، والديني[28].

وبقدر تعلق الأمر بموضوع بحثنا، فإن المواقع الإلكترونية التي يقوم المستخدم بزيارتها، وأهمها مواقع التواصل الاجتماعي تستخدم تقنية ملفات تعريف الارتباط أو الكوكيز Cookies، التي هي ملفات نصية ترسل وتخزن في القرص الصلب للجهاز الإلكتروني الخاص بالمستخدم، وتحتوي على معلومات شخصية معينة عن المستخدم كعنوان بروتوكول الإنترنت «IP» الخاص به، وطريقة الاتصال بالإنترنت، والمواقع التي يقوم بزيارتها، ونوع الجهاز ونوع المعالج، ويحتفظ الموقع الذي تتم زيارته بنسخة من هذه المعلومات. صحيح أن مثل هذه المعلومات تسهل زيارة المستخدم للمرة الثانية للموقع ذاته والحصول على أدق التفاصيل، غير أن خطورة تلك المعلومات الشخصية عن المستخدم تكشف عن خطوات واتجاهات المستخدم، ومعرفة المواقع التي يزورها

(27) د. منى الأشقر جبور ود. محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، ط1، جامعة الدول العربية، بيروت، 2018، ص22.

(28) المرجع السابق، ص22.

المستخدم، ومعرفة سلوكه بشكل عام، مما يجعله عرضة دائماً لتوجيه الإعلانات التجارية له والتي تناسبه من قبل الشركات. كما أنه من الممكن سرقة ملفات تعريف الارتباط الخاصة بالمستخدم واستخدام المعلومات الواردة فيها بدلاً من المستخدم، بما يتيح اختراق الصفحات الشخصية التي تخص المستخدم، وفي هذا تهديد واضح لخصوصية المستخدم[29].

الفرع الثاني

الرابط بين الخصوصية والاستخدام المشروع

نشير في هذا الموضع إلى الحكم الصادر من محكمة لوكسمبورج لغرض تحديد العلاقة بين مسألة الخصوصية والاستخدام المشروع للمواد والأجهزة الإلكترونية، ففي القضية المعروفة باسم Sabam vs. Scarlet ISP وهو اختصار لشكوى الرابطة البلجيكية للمؤلفين والملحنين والناشرين ضد مزود خدمة الإنترنت، طالبت الرابطة البلجيكية من محكمة لوكسمبورج إلزام مزود خدمة الإنترنت بوضع نظام فلترة يمكنه منع ومراقبة الأجهزة من خلال عنوان بروتوكول الإنترنت «IP» الخاص بالعملاء في استخدام وتنزيل المواد المحمية بحقوق التأليف.

وقد قضت المحكمة البلجيكية لصالح المدعي وألزمت مزود خدمة الإنترنت بذلك، إلا أن المدعى عليه، والذي هو مزود خدمة الإنترنت، طعن على الحكم أمام محكمة الاستئناف في بروكسل، ووجهت هذه المحكمة سؤالاً إلى محكمة العدل الأوروبية فيما إذا كان تشريع الاتحاد الأوروبي يسمح للمحاكم الوطنية أن تأمر بتركيب أنظمة فلترة على الاتصالات الإلكترونية بين الأجهزة، وقد قررت محكمة العدل الأوروبية بأن إلزام مزود خدمة الإنترنت لا يتوافق وتشريع الاتحاد الأوروبي، وأن من شأن ذلك التعارض مع حقوق مستخدمي شبكة الإنترنت مع عدم إهمال حق المستخدمين في حماية بياناتهم الشخصية[30].

إذن، فالعلاقة بين حماية الحق في الخصوصية وحرية الوصول إلى المعلومات ينبغي أن يكون فيها نوع من التوازن، بحيث يكون من حق مستخدم الإنترنت استخدام الشبكة، ولكن بشكل مشروع لكي يكفل بذلك حماية خصوصيته.

---

(29) د. عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مجلة جامعة طنطا، كلية الحقوق، دون رقم عدد، دون تاريخ نشر، ص14.

(30) القرار منشور على الموقع الإلكتروني: https://zuniclaw.com/en/ip-address-personal–data/ تاريخ الزيارة 2020/2/25.

وعلى هذا، يصطدم الحق بالخصوصية بعائق يتمثل في ضرورة الاستخدام المشروع لشبكة الإنترنت والأجهزة الإلكترونية المتصلة بها، لذلك فإننا نجد بأن شركات مزودي خدمات الإنترنت ومحركات البحث مضطرة أحياناً للكشف عن هوية المستخدم، وانتهاك خصوصيته فيما لو قام الأخير بجرائم إلكترونية من قذف وتشهير وابتزاز وأعمال إرهابية، أو بث مواد إباحية للأطفال وغير ذلك.

فالأولوية هنا ينبغي أن تعطى لحق تلك الشركات في ضرورة قيام المستخدم باستعمال الأجهزة الإلكترونية استخداماً مشروعاً، وهنا نستطيع القول: «تنتهي الخصوصية حينما يبدأ الاستخدام غير المشروع للإنترنت والأجهزة الإلكترونية».

المبحث الثاني
الأبعاد القانونية للمرحلة اللاحقة للكشف عن عنوان بروتوكول الإنترنت «IP address»

الخصوصية حق إنساني أصيل، ورُكن أساسي لقيام المجتمعات الديمقراطية، وهي جوهرية لحفظ الكرامة الإنسانية، كما تُعضّد حقوقاً أخرى مثل حرية التعبير والحصول على المعلومات وحرية التنظيم، ويُقرّها قانون حقوق الإنسان الدولي، وإن مراقبة الاتصالات تنتقص من الحق في الخصوصية ومن حقوق إنسانية أخرى، لذا لا يمكن تبريرها إلا إذا كان منصوصًا عليها في القانون، وضرورية لتحقيق غرض مشروع، ومتناسبة مع الغرض المنشود[31].

إن الكشف عن عنوان بروتوكول الإنترنت «IP address» لا يكون إلا لغرض يجيزه القانون، وإذا كان من شأن الكشف عن عنوان بروتوكول الإنترنت انتهاك الخصوصية عرضاً، فإن المسؤولية قد تقع على مستخدم الإنترنت في إساءة استعمالها واستعمال الأجهزة المتصلة بها. وفيما عدا ذلك، فإن الكشف عن تلك العناوين يثير بلا شك المسؤولية القانونية؛ وهذا ما سنحاول تبيينه في المطلبين الآتيين:

المطلب الأول
مسؤولية الشخص عن تتبع عناوين بروتوكول الإنترنت «IP address»

قد يكون من المشروع قانوناً تتبع عناوين بروتوكول الإنترنت «IP» للهواتف المحمولة وأجهزة الكمبيوتر والطابعات العائدة لبعض المستخدمين، كما في حالة قيام مستخدمي الشبكة بارتكاب بعض الجرائم من خلالها – والتي سنشير إليها في الفرع الثاني– غير أن تعقب الأشخاص عن طريق عنوان بروتوكول الإنترنت «IP» قد يكون في حد ذاته جريمة حينما يتعلق الأمر بانتهاك خصوصية الشخص والكشف عن بياناته، خاصة وإن تم ذلك من خلال أجهزة الشرطة، مما قد يكون أداة مراقبة قمعية للغاية.

(31) ديباجة المبادئ الدولية والضرورية Necessary and proportionate principles لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتصالات، النسخة النهائية، آيار/مايو 2014. لاحظ الموقع الإلكتروني الخاص بالمبادئ necessaryandproprtionate.org/principles تاريخ الزيارة للموقع: 2020/5/13. جدير بالذكر أنه شارك أكثر من 400 من خبراء الخصوصية والأمن في عملية صياغة المبادئ في اجتماع في بروكسل في أكتوبر 2012، وقد قادت عملية صياغة تعاونية استندت إلى خبرات العديد من خبراء الخصوصية الدولية Privacy International وحقوق الإنسان والحقوق الرقمية من مختلف أنحاء العالم.

فلابد من الحذر من أن استخدام هذه التقنية لا تكون إلا لغرض محدد، وبخلافه يتحمل الشخص المسؤولية الكاملة عن انتهاك الخصوصية كأحد حقوق الإنسان[32]. ففي إحدى القضايا؛ نشر فني صوراً مهينة لإحدى الشخصيات التاريخية على موقع الفيسبوك، وتعرفت عليه الشرطة من خلال عنوان بروتوكول الإنترنت «IP» الذي تم الحصول عليه من موقع جوجل Google ومزود خدمة الإنترنت Airtel وتم حبس المتهم 50 يوماً، ثم اكتشف فيما بعد أن مزود خدمة الإنترنت قدم للسلطات عنوان بروتوكول إنترنت «IP» خاطئ، ذلك لأن هذه الشركة لم تتحقق فيما إذا كان المشتبه به قد نشر المحتوى في الساعة 1:15 مساء أم لا. ولهذا ألزمت اللجنة الحكومية لحقوق الإنسان بدفع تعويض للمتضرر قيمته 200 روبية[33].

ومن الجدير بالذكر أن المسؤول عن تتبع عناوين بروتوكول الإنترنت «IP» الخاص بالمستخدمين غالباً ما يكون متمثلاً بموقع إلكتروني على شبكة الإنترنت يُدار من قبل شخص معين أو شركة معينة[34]، وعند زيارة هذا الموقع فإنه يتم وضع ملف صغير على القرص الصلب لجهاز الكمبيوتر الخاص بالمتصفح أو هاتفه المحمول، بحيث يتصل بالخادم الخاص بالموقع الذي تتم زيارته عبر الشبكة، ومن خلال هذا الخادم يتم بث معلومات وملفات إلى كمبيوتر المستخدم ويحتفظ بنسخة من تلك الملفات، ومن هنا يتعرض المستخدمون لخطر انتهاك خصوصياتهم وجمع المعلومات عنهم خلال تصفحهم للمواقع، حيث يستطيع ما يسمى بالبوصلة التقنية المعروفة بـ (كوكيز cookies) معرفة عنوان بروتوكول الإنترنت «IP» للمستخدم، وطريقة اتصاله بالإنترنت والمواقع التي زارها[35].

وحماية للمستخدم من هذا الخطر، فإن المواقع الإلكترونية ملزمة الآن – بموجب التوجيهات والقوانين المتعلقة بالخصوصية وحماية البيانات الشخصية – بالإعلام أو الإدلاء بالبيانات للمستخدم، بأنها تستخدم الـ (كوكيز) حتى يكون المستخدم على دراية

(32) تنص المادة (17) من دستور العراق لسنة 2005 على أنه: «لكل فرد الحق في الخصوصية الشخصية، بما لا يتنافى مع حقوق الآخرين والآداب العامة».

(33) Prashant Iyengar, Ip address and expeditious disclosure of identity in india, research available at: www.cis-india.org, Last accessed on: 19/3/2020.

(34) ونظراً للضغوط الدولية بشأن ضرورة حماية الحق في الخصوصية المعلوماتية، وخاصة بعد صدور نظام الاتحاد الأوروبي لحماية البيانات لسنة 2018، فقد قامت شركة أبل Apple بإطلاق موقع جديد على أجهزتها للبيانات والخصوصية Privacy Portal، مما يتيح للمستخدم إمكانية تنزيل كل ما تقوم به الشركة بربطه شخصياً بحسابات المستخدمين، من معلومات Apple ID وapple care ونشاط app store إلى البيانات المخزنة في iCloud مثل الصور والمستندات.

(35) د. أحمد محمد المعداوي، مرجع سابق، ص1964.

كافية في كيفية السيطرة على معلوماته واستخدامها. ولتحقيق وتنفيذ هذا الالتزام، فإنه درج الحال الآن على كتابة عبارة «نحن نستعمل كوكيز في موقعنا الإلكتروني» أو (we use cookies)، وإلا فإن الإخلال بهذا الالتزام يوجب المسؤولية والتعويض عن أي ضرر يلحق بالمستخدم جرَّاء معالجة بياناته الشخصية وكشف هويته.

تجدر الإشارة إلى أن مكتب التحقيقات الفيدرالي الأمريكي أصدر بتاريخ 2019/11/26 تحذيراً للمستخدمين من مخاطر أجهزة التلفزيونات الذكية Smart TV المزودة بميكرفون وكاميرا، إذ تتيح للمصنعين جمع البيانات عن عادات العائلات في استخدام جهاز التلفزيون، وأيضاً التعرف على أفراد العائلة إذا كان التلفزيون مزوداً بتقنية التعرف على الوجه. فكل جهاز متصل بالإنترنت يكون له عنوان بروكول إنترنت «IP» خاص بالمستخدم، مما يتيح التعرف على هوية المشاهد[36].

أما بالنسبة لنوع المسؤولية التي تقوم بحق من يتتبع عناوين بروتوكول الإنترنت، فهي إما تكون تعاقدية فيما لو كان الاعتداء على البيانات الشخصية قد حدث من قبل مزودي خدمة الإنترنت أو مزودي خدمة الاتصال بالشبكة، إذ غالباً ما تربطهم علاقة تعاقدية مع المستخدمين، وتسمى بعقود الاشتراك في خدمات الاتصالات أو الإنترنت[37].

وبموجب هذا العقد يلتزم مزود خدمة الإنترنت، أو مزودو خدمة الاتصال بشبكة الإنترنت، بالسرية وحماية خصوصية المستخدم أو المشترك[38]، فهذا النوع من العقود يتطلب إفضاء المشترك بمجموعة من البيانات الشخصية بشكل مباشر أو غير مباشر أثناء إبرام العقد، بحيث يتعرض لخطر قيام مقدم الخدمة بإفشاء هذه البيانات، مما يسهل كشف هويته بعد التعرف على ميوله ورغباته خلال تتبع استخدامه للهاتف أو جهاز الكمبيوتر أو الانترنت.

(36) نايلة الصليبي، تحذير مكتب التحقيقات الفدرالي للمستخدمين من مخاطر الاختراقات الأمنية لأجهزة التلفزيونات الذكية المتصلة Smart TV، مقال على موقع مونتي كارلو الدولية، تاريخ النشر: 2019/12/5، متاح على الموقع: https://www.mc-doualiya.com، تاريخ الزيارة، 2019/12/9.

(37) تنص المادة (74) من التوجيه الأوروبي العام لحماية البيانات لسنة 2016 وتحت عنوان: (مسؤولية مراقب المعلومات أو حارسها) على أنه: «1- يجب تحديد مسؤولية المتحكم عن أي معالجة للبيانات الشخصية، سواء تمت من قبل المتحكم المراقب نفسه أو نيابة عنه 2- وعلى وجه الخصوص يلزم المراقب باتخاذ تدابير مناسبة وفعَّالة، وأن يكون قادراً على إثبات امتثال هذه المعالجة للمعلومات للائحة بما في ذلك فعالية التدابير 3- يجب أن تأخذ هذه التدابير في الاعتبار طبيعة ونطاق وسياق وأغراض المعالجة والمخاطر على حقوق وحريات الأشخاص الطبيعيين».

(38) وسند هذا القول ما نصت عليه المادة (4) من القانون الفرنسي 2004/669 الخاص بالاتصالات الإلكترونية وخدمات الاتصال المرئية. وكذلك المادة (47) من مشروع قانون هيئة الإعلام والاتصالات العراقي لسنة 2017 ونصها: «تعتبر المكالمات الهاتفية والاتصالات الخاصة من الأمور السرية، التي لا يجوز مراقبتها أو التنصت عليها أو الكشف عنها، إلا لضرورة قانونية وأمنية، وبقرار قضائي».

وبالطبع يعد كل ما يتعلق بعنوان بروتوكول الإنترنت من قبيل البيانات الشخصية. وهنا يمتنع على مقدمي خدمة الإنترنت إفشاء هذه البيانات أو معالجتها أو استخدامها بأية طريقة دون موافقة صاحبها، إلا إذا كان الغرض من الاحتفاظ بها أو معالجتها هو المصلحة العامة أو تحسين الخدمات المقدمة. أما عن طبيعة هذا الالتزام، فنعتقد أنه التزام بنتيجة، فعلى مقدمي خدمة الإنترنت والاتصال اتخاذ التدابير اللازمة لمنع إفشاء البيانات الخاصة بالمستخدمين.

وبالتالي تكون هذه الجهات مسؤولة مسؤولية عقدية، إذا لم تحقق النتيجة المطلوبة للمستخدم والذي يعد دائناً في العلاقة التعاقدية، ولا تستطيع هذه الجهات التخلص من المسؤولية، الا إذا أثبتت بأن عدم تحقق النتيجة (الامتناع عن إفشاء المعلومات) قد حصل بسبب أجنبي، كأن تكون هناك مشكلة تقنية أدت لنشر تلك البيانات[39].

ولكن يجب التنويه هنا أن الالتزام بالامتناع عن إفشاء المعلومات الخاصة بالمستخدمين ليس التزاماً مطلقاً، بل ترد عليه استثناءات، كما لو قامت تلك الجهات بكشف تلك البيانات تنفيذاً للقوانين، أو بناءً على طلب من سلطة قضائية مختصة، وذلك للأغراض الأمنية من تتبع المجرمين وغير ذلك. ويلاحظ هنا أن التعويض في المسؤولية العقدية يقتصر على الضرر المادي دون الأدبي، ويشترط في الضرر المادي أن يكون متوقعاً، إلا إذا ارتكب المدين بالالتزام غشاً أو خطأً جسيماً، حينها يلزم بتعويض الضرر كله متوقعاً أو غير متوقع[40].

أما لو كان الاعتداء على عناوين بروتوكول الإنترنت قد حصل من قبل الغير (شخص ثالث)، كمستخدم آخر للشبكة، فالمسؤولية تكون بالطبع تقصيرية. وبالرغم من أن القانون المدني العراقي رقم 40 لسنة 1951 لم ينظم الحق في الخصوصية، لكن هذا لا يعني عدم إمكانية إسناد هذه المسؤولية للقواعد العامة، حيث تنص المادة (204) من القانون المدني العراقي على أن: «كل تعد يصيب الغير بأي ضرر آخر غير ما ذكر في المواد السابقة يستوجب التعويض».

وعلى هذا تستند المسؤولية وفقاً لهذا النص على فكرة التعدي، وهذا ما يسميه البعض[41] بخطأ التعدي على الخصوصية. وبالطبع يقوم خطأ الفاعل حينما يستخدم تقنية عنوان

(39) المادتان (168) و(169) من القانون المدني العراقي. وأيضاً: د. محمد سليمان الأحمد، الخطأ وحقيقة أساس المسؤولية المدنية في التشريع العراقي، مكتب التفسير، أربيل، 2008، ص15.

(40) المادة (3/169) من القانون المدني العراقي.

(41) د. يونس صلاح الدين علي، المسؤولية المدنية الناجمة عن التعدي على الحق في الخصوصية في القانون الإنجليزي: دراسة تحليلية مقارنة بالقانون الإنجليزي، مجلة الحقوق، الجامعة المستنصرية، العراق، المجلد 1، الاصدار 29–30، سنة 2017، ص24.

بروتوكول الإنترنت «IP» في انتهاك الالتزام القانوني بالمحافظة على سرية المراسلات، التي تتضمن بيانات شخصية عن المستخدم تتسم بالسرية، أو أن لها طابع الخصوصية، وكل ذلك يتم دون موافقة المستخدم.

وقد لا يقترن فعل الفاعل بالتعمد عند كشف خصوصية المستخدم من خلال عنوان بروتوكول الإنترنت. ونشير أيضاً إلى أن انتهاك خصوصية المستخدم قد يتم مباشرة أو تسبباً، فالفاعل (المتحكم بالمعلومات) يكون مباشراً في إحداث الضرر بالمستخدم حينما يكشف السرية بنفسه، وقد يتسبب الفاعل في إحداث الضرر كما لو توسط بين فعله والضرر الذي لحق بالمستخدم فعل المباشر، كأن يكون معالج المعلومات قد حصل من خلال عنوان بروتوكول الإنترنت «IP» على بيانات شخصية للمستخدم، وأهمل في المحافظة عليها، أو قام بخزنها لمدة طويلة، فوصلت إلى شخص ثالث قام بنشرها وكشف هوية المستخدم ومراسلاته، فهنا يكون من حصل على المعلومات متسبباً في إحداث الضرر، ومن قام بنشرها مباشراً[42].

وفيما يتعلق بأثر المسؤولية التقصيرية ألا وهو التعويض، فقد نصت المادة (205) من القانون المدني العراقي على أنه: «يتناول حق التعويض الضرر الأدبي كذلك، فكل تعد على الغير في حريته أو في عرضه أو في شرفه أو في سمعته أو في مركزه الاجتماعي أو في اعتباره المالي يجعل المعتدي مسؤولاً عن التعويض». ومن هذا النص نستنتج أن استخدام عنوان بروتوكول الإنترنت وتأثيره على الخصوصية، إذا كان من شأنه أن يلحق ضرراً مادياً أو معنوياً بالمستخدم، فإنه يوجب التعويض سواء أكان الضرر متوقعاً أم غير متوقع.

أما بالنسبة لنظام حماية البيانات الأوروبي لسنة 2016، فقد عالج التعويض بصفة عامة، فجاءت المادة (78) لتوضح أن من حق أي شخص طبيعي أو معنوي أن يطلب التعويض بموجب شكوى من السلطة المشرفة على حماية البيانات الشخصية. أما المادة (79) فذهبت إلى أنه: «يحق لصاحب البيانات إضافة لحقه في تقديم شكوى، طلب تعويض قضائي فعَّال من المحكمة، فيما لو رأى أن حقوقه انتهكت نتيجة معالجة بياناته الشخصية خلافاً للنظام».

ونصّت المادة (1/81) من النظام على أنه: «يكون للشخص الذي عانى من أضرار مادية أو غير مادية كنتيجة للإخلال بهذا النظام، الحق في الحصول على التعويض من وحدة التحكم بالبيانات، أو معالج البيانات عن الأضرار التي لحقت به». وعن نفي المسؤولية

(42) المادة (186) من القانون المدني العراقي. وأيضاً: د. محمد سليمان الأحمد، مرجع سابق، ص59.

نصت الفقرة الثالثة من المادة (81) على أنه: «يتم إعفاء وحدة التحكم بالبيانات أو المعالج من المسؤولية، إذا ثبت أنها ليست مسؤولة بأي حال عن الفعل الذي تسبب في إحداث الضرر»[43].

وتحدثت الفقرتان الرابعة والخامسة من المادة نفسها عن موضوع التضامن بين المدينين في تحمل المسؤولية كما هو معروف في القوانين المدنية، حيث نصتا على أنه: «عندما يكون أكثر من وحدة تحكم أو معالج أو كليهما متورطين في المعالجة للبيانات، وحيث يكونان مسؤولين عن أي ضرر نتيجة المعالجة، تكون كل وحدة تحكم أو معالج مسؤولة عن الضرر بأكمله من أجل ضمان التعويض الفعَّال لصاحب البيانات، وإذا دفع معالج أو وحدة التحكم التعويض الكامل، يحق له الرجوع على وحدات التحكم الأخرى أو المعالجين الآخرين، بالتعويض الذي يقابل مساهمته ومسؤوليته في إحداث الضرر».

المطلب الثاني

مسؤولية مستخدم الجهاز عن الأعمال غير المباحة التي أتاحت للغير معرفة عنوان بروتوكول الإنترنت «IP address»

يُثار التساؤل حول الأسباب التي تدعو مواقع الإنترنت إلى ضرورة الكشف عن عنوان بروتوكول الإنترنت للمستخدمين وتحديد هوياتهم، والمسألة لا تخرج عن اقتضاء المصلحة العامة في منع الضرر والجرائم الإلكترونية، كالابتزاز والتشهير والاحتيال المالي، أما الكشف عن تلك الهوية لغير الأغراض السابقة فيعد انتهاكاً واضحاً للحق في الخصوصية وحماية البيانات الشخصية.

وهنا نشير إلى أهم تلك الأسباب من خلال تجارب بعض الدول، ففي الهند[44] بوصفها تحوي أكثر مستخدمي الإنترنت لغاية عام 2016، حصلت عدة وقائع أدت لضرورة التحري عن بعض مستخدمي الشبكة، وذلك من خلال الاستعانة بعنوان بروتوكول الإنترنت «IP»، فمثلاً في شهر أيار/مايو من عام 2010 تم اعتقال ضابط في الشرطة في مدينة مومباي الهندية لتوزيعه مواد إباحية للأطفال من خلال جهاز الكمبيوتر الخاص به، وتم تتبعه بعد أن نبهت الأنتربول السلطات الهندية بأن الصور الإباحية كان يتم

(43) وهذا مضمون المادة (211) مدني عراقي نفسها إذ جاء فيها: «إذا أثبت الشخص أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه ... كفعل الغير كان غير ملزم بالضمان ما لم يوجد نص أو اتفاق على غير ذلك».

(44) جدير بالذكر أنه نظراً لحداثة موضوع عنوان بروتوكول الإنترنت «IP»، والذي بدأت تتضح معالمه منذ عام 2016، فإننا لم نعثر على قرارات للمحاكم العراقية والمصرية بهذا الخصوص.

تحميلها من عنوان بروتوكول الإنترنت «IP» الذي كان يستخدمه.

وفي عام 2008 ألزمت المحكمة العليا في مومباي بالهند إحدى شركات البحث على الإنترنت بالكشف عن تفاصيل وعنوان واسم الشخص الذي نشر محتوى تشهيرياً بحق شركة المدونات الخاصة التابعة لجوجل Google blogger. وفي شهر شباط/ فبراير من عام 2011 تتبعت الشرطة صبياً مفقوداً كان قد هرب من المنزل، وذلك باتباع مسار عنوان بروتوكول الإنترنت «IP» الذي غادره عند تحديثه لحالة ملفه الشخصي على موقع الفيسبوك Facebook[45].

وتُثار بهذا الشأن مسؤولية مستخدم الهاتف النقال في اتصاله بالإنترنت عن إساءة استخدام هذا الجهاز، مما يتيح عملية الكشف عن الهوية وعنوان بروتوكول الإنترنت «IP»، وذلك كلما قام بفعل الذم والقدح والتحقير، سواء أكان في شكل صور أم رسائل أم محادثات صوتية من الهاتف النقال وإليه، وكذلك إزعاج ومضايقة الغير والتعرض لهم، وتصوير شخص دون رضاه، وبث الصورة من خلال أجهزة شبكة الإنترنت، فضلاً عن بث الرسائل غير المرغوب بها[46]. وهنا من الممكن اللجوء إلى القواعد العامة في المسؤولية المدنية[47] والقوانين الخاصة بهذا الشأن[48].

وفي الواقع نجد أن هناك الكثير من الأعمال غير المباحة التي تمارس من قبل مستخدمي الأجهزة الإلكترونية، سواء على مواقع التواصل الاجتماعي وتحديداً فيسبوك Facebook أو بواسطة أجهزة الهاتف النقال المرتبطة بالإنترنت. فتجد أحياناً أن الشخص يقوم بإرسال رسائل التهديد لآخر أو نشر رسائل منافية للآداب، أو نشر صور أو رسائل

(45) Prashant Iyengar, IP Addresses and Expeditious Disclosure of Identity in India, ce - ter for internet and society, paper available at: https://cis-india.org/internet-governance/resources, published in 22 August 2011, Last accessed on: 3-12-2019.

(46) أروى محمد تقوى، مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالإنترنت، مجلة الحقوق، جامعة البحرين، المجلد 11، العدد 2، سنة 2014، ص370 وما بعدها.

(47) لاحظ على سبيل المثال المادة (6) والمادة (204) من القانون المدني العراقي رقم 40 لسنة 1951 المعدل.

(48) على سبيل المثال جاء في المادة (2) من قانون منع إساءة استعمال أجهزة الاتصالات في إقليم كوردستان– العراق رقم 6 لسنة 2008 على أنه: «يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن مليون دينار ...: كل من أساء استعمال الهاتف الخلوي، أو أية أجهزة اتصال سلكية أو لا سلكية، أو الإنترنت أو البريد الإلكتروني، وذلك عن طريق... نشر معلومات تتصل بأسرار الحياة الخاصة أو العائلية للأفراد، والتي حصل عليها بأية طريقة كانت ولو كانت صحيحة، إذا كان من شأن نشرها وتسريبها وتوزيعها الإساءة اليهم أو إلحاق الضرر بهم».

لإثارة الفزع أو الفتن. كذلك جرائم الابتزاز المالي[49]، واختراق حساب الغير أو انتحال الشخصية. فكل هذه الأنشطة تكون مدعاة لتدخل السلطة العامة، والطلب من مزود خدمة الإنترنت بكشف عنوان بروتوكول الإنترنت «IP» الخاص بالمستخدم، حفاظاً على الأمن العام للمجتمع من جهة وخصوصيات الآخرين من جهة أخرى.

ونعتقد بأن إخفاء المستخدم لهويته من شأنه إلحاق الضرر بالغير، ففي قضية قامت سيدة مستخدمة لشبكة الإنترنت بإخفاء هويتها وبحساب وهمي، وراسلت ابنة صديقتها السابقة من خلال البريد الإلكتروني وأخطرتها بأن العالم سيكون أفضل من دونها، مما أدى ذلك بالفتاة إلى الانتحار، وتمت إدانة المدعى عليها بسبب إخفائها لهويتها، وسوء استخدامها ودوافعها لفتح حساب على الشبكة[50].

ولا شك في أن المسؤولية التي تُثار ضد مستخدم الشبكة هي مسؤولية تقصيرية، فلا تربطه علاقة تعاقدية مع الشخص المعتدي على بياناته الشخصية، وفي هذا من الممكن اللجوء إلى القواعد العامة في المسؤولية المدنية المتعلقة بالفعل الضار والضرر ورابطة السببية، لكي يتحقق أثر المسؤولية تلك ألا وهو التعويض، سواء أكان تعويضاً نقديا أم عينياً.

ووفقاً لما تقدم يتعين على كل المستخدمين عند بحثهم عن المعلومات أن يحترموا حقوق الغير كحق الملكية الفكرية والحقوق المتعلقة بالحياة الخاصة والحق في النسيان الرقمي[51]. وبالرغم من أن البعض يذهب إلى القول بعدم مسؤولية مستخدم الإنترنت نهائياً كونه لا يخضع لأي قيد أو شرط وهو في فضاء الإنترنت، إلا أن المستقر عليه هو أن المستخدم يجب أن يبذل عناية الشخص الحريص وهو يزاول نشاطه عبر الإنترنت[52].

---

(49) د. محمد عبد الوهاب المحاسنة، المسؤولية المدنية عن انتهاك الخصوصية في وسائل الاتصال الإلكترونية وفقاً للقانون الأردني، مجلة كلية الشريعة والقانون بتفهنا الأشراف، دقهلية، مصر، المجلد 20، العدد 1، 2018، ص 687.

(50) Jennifer Steinhauer, Verdict in MySpace Suicide Case, nov., 2008, New York times journal, https://www.nytimes.com/2008/11/27/us/27myspace.html, Last accessed on: 12-03-2020.

(51) https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr, Last accessed on:: May 14, 2020.

«ويُقصد بالحق في النسيان الرقمي، حق مستخدم الإنترنت في المحافظة على ماضيه الرقمي، وبقائه في حيز النسيان والسيطرة على معلوماته التي مضت فترة زمنية على بثها عبر الإنترنت مع محوها آلياً من قبل محركات البحث عند تركه مراجعتها خلال فترة يحددها هو بنفسه مسبقاً عند بثه للمعلومة». الزين بوخلوط، الحق في النسيان الرقمي، مجلة المفكر، العدد14، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر، ص590 وما بعدها.

(52) د. محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003، ص 239.

الخاتمة

وتتضمن أهم النتائج والتوصيات:

أما بالنسبة للنتائج فهي:

1- تعد عناوين بروتوكول الإنترنت «IP» معلومات شخصية؛ لأنها معلومات عن فرد محدد يرتبط بها؛ ولهذا فإن للفرد الحق في معرفة المعلومات التي يتم تخزينها عنه، وفيما سيتم استخدامها من خلال تقنية عنوان بروتوكول الإنترنت «IP»، وكل ذلك بعد الحصول على موافقة صريحة منه بعمل ذلك.

2- ضرورة الاستخدام المحدد لتكنولوجيا الكشف عن البيانات الشخصية للفرد من خلال عنوان بروتوكول الإنترنت «IP»؛ لما في ذلك من خطر يتعلق بانتهاك حقوق الإنسان.

3- إن الكشف عن عناوين بروتوكول الإنترنت «IP» الخاصة بالمستخدم، وانتهاك خصوصيته يتم إما من قبل مزودي خدمات الإنترنت، أو محركات البحث ومواقع الويب من خلال الاستعانة بطرف ثالث.

4- إن المتفق عليه في توجيهات الاتحاد الأوروبي هو أن عناوين بروتوكول الإنترنت «IP» يتم تكييفها على أنها من قبيل المعلومات الشخصية التي ينبغي أن تتمتع بالحماية نفسها التي تتمتع بها تلك المعلومات. فمن الجائز قانوناً تخزين تلك المعلومات لأغراض محددة، أما بعد ذلك فينبغي محوها وإزالتها من شبكة الإنترنت، وهذا قد يكون تطبيقاً لما يسمى بحق الإنسان في النسيان الرقمي.

5- لا يجوز لشركات الاتصالات ومحركات البحث الإلكترونية مشاركة البيانات الشخصية للشخص المستخدم للجهاز الإلكتروني المرتبط بشبكة الإنترنت مع طرف ثالث، إلا بعد الحصول على موافقة صاحب تلك البيانات أو إخطاره بذلك.

وفيما يتعلق بالتوصيات:

نشير إلى ضرورة إضافة هذه النصوص للقوانين التي تتعامل مع أنشطة الاتصال واستخدام الهواتف وغيرها:

1- لا تكون مراقبة الاتصالات وتخزين البيانات الشخصية والإفصاح عنها لمستخدم الشبكة والأجهزة المتصلة بها مشروعاً إلا للأغراض التالية:

أ. منع أو الكشف عن جريمة بناءً على طلب تحريري من الجهات الرسمية.

ب. إذا كان القانون أو القضاء يتطلب الكشف عن تلك البيانات.

2- لا يجوز لمزودي خدمات الإنترنت أو الاتصال ومحركات البحث ومواقع التواصل الاجتماعي تخزين البيانات الشخصية الخاصة للمستخدم والمتعلقة بالأسرة، أو بالسجل الإجرامي القديم، أو السمعة المالية من خلال ملفات الكوكيز وعناوين بروتوكول الإنترنت، إلا لأغراض الأمن العام والمصلحة العامة، كما يجب على تلك الجهات حذف تلك البيانات فيما لو طلب منها ذلك، إذا لم تعد تلك المعلومات ضرورية، أو أنها خزنت دون مبرر قانوني، باستثناء المعلومات التي تكون في شكل مصنفات أدبية منشورة، أو تلك التي تجسد حق التعبير والوصول للمعلومات.

المراجع

أولاً- باللغة العربية

1- الكتب

- د. هانيا فقيه دندش، دراسات في القانون الخاص، 5- حماية الحق في الخصوصية المعلوماتية، الجزء الأول، ط1، منشورات زين الحقوقية، بيروت، 2019.
- د. محمد حسين منصور، المسؤولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، 2003.
- د. محمد سليمان الأحمد، الخطأ وحقيقة أساس المسؤولية المدنية في التشريع العراقي، مكتب التفسير، أربيل، العراق، 2008.
- د. محمد عبد الوهاب المحاسنة، المسؤولية المدنية عن انتهاك الخصوصية في وسائل الاتصال الإلكترونية وفقاً للقانون الأردني، مجلة كلية الشريعة والقانون بتفهنا الأشراف، دقهلية، مصر، المجلد 20، العدد 1، سنة 2018.
- د. منى الأشقر جبور و د. محمود جبور، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، ط1، جامعة الدول العربية، بيروت، 2018.

2- البحوث

- الزين بوخلوط، الحق في النسيان الرقمي، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، الجزائر، العدد 14.
- أروى تقوى،
  - الغفلية على الإنترنت بين سندان الحق في الخصوصية ومطرقة المسؤولية، مجلة المنارة للبحوث والدراسات، جامعة آل البيت، الأردن، المجلد 20، العدد 1، سنة 2014.
  - مدى مسؤولية مشغلي الهاتف النقال عن إساءة استخدامه في الاتصال بالإنترنت، مجلة الحقوق، جامعة البحرين، المجلد 11، العدد 2، سنة 2014.
- د. يونس صلاح الدين علي، المسؤولية المدنية الناجمة عن التعدي على الحق في الخصوصية في القانون الإنجليزي: دراسة تحليلية مقارنة بالقانون الإنجليزي، مجلة الحقوق، الجامعة المستنصرية، العراق، المجلد 1، الإصدار 29-30، سنة 2017.

- د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية عبر شبكات التواصل الاجتماعي، بحث متاح على الرابط الإلكتروني: https://mksq.journals.ekb.eg/article_30623_1ab2f80af612aa4568dbf6239b535ac2.pdf.
- د. منى تركي الموسوي وجان سيريل فضل الله، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بمؤتمر الكلية، 2013.
- مصطفى عائشة بن قارة ، الحق في الخصوصية المعلوماتية بين التحديات التقنية وواقع الحماية القانونية، المجلة العربية للعلوم ونشر الأبحاث، المجلد الثاني، العدد 5، سنة 2016.
- نايلة الصليبي، تحذير مكتب التحقيقات الفدرالي للمستخدمين من مخاطر الاختراقات الأمنية لأجهزة التلفزيونات الذكية المتصلة TV Smart، موقع مونتي كارلو الدولية، تاريخ النشر: 2019/12/5، متاح على الموقع: https://www.mc-doualiya.com
- د. سوز حميد مجيد، الحماية القانونية للحق في خصوصية البيانات الشخصية في العراق، مجلة دراسات قانونية وسياسية، جامعة السليمانية، السنة السادسة، العدد 11، نيسان/أبريل 2018.
- د. عبد الكريم صالح عبد الكريم، تدابير الحماية التكنولوجية ودورها في حماية المصنفات الرقمية: دراسة تحليلية مقارنة، مجلة الحق، جمعية الإمارات للمحامين والقانونيين، العدد 17، 2013.
- د. عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مجلة جامعة طنطا، كلية الحقوق، دون بيانات رقم العدد، دون تاريخ النشر.
- رنا أبتر، خرائط غوغل تتبعك أينما كنت، صحيفة الشرق الأوسط، 19 كانون الأول/ديسمبر 2019، العدد 14996.

ثانياً- باللغة الإنجليزية

1- Books

- Daniel Felz, ECJ Declares IP Addresses are Personal Data, October 19, 2016.
- Stuart Hargreaves and lokman Tsui, IP address as personal data under Hong Kong privacy law, an introduction to the access my info HK project, the Chinese university of Hong Kong faculty of law research paper no.2017-23, journal of information, law & science 25(2).

2- Research

- Eneken Tikk, IP addresses subject to personal data regulation, Paper available at: https://ccdcoe.org.
- Frederick Lah, Are Ip address personally identifiable information? Journal of law and policy for information society, vol.4:3, 2008.
- Hustinx, Nameless Data Can Still be Personal, Out-Law.Com, Nov. 6, 2008, http://www.out-law.com/page-9563.
- Jennifer Steinhauer, Verdict in MySpace Suicide Case, nov, 2008, New York times journal, https://www.nytimes.com/2008/11/27/us/27myspace.html.
- KIM porter, Are VPNs legal or illegal? Paper available at: https://us.norton.com/internetsecurity-privacy-are-vpns-legal.html.
- Meryem Marzouki, Is the IP Address Still a Personal Data in France? European Digital Rights, Sept. 12, 2007, http://www.edri.org/edrigram/number5.17/ip-personal-data-fr.
- Pinsent Masons, Out-Law-Guide, IP addresses and the Data Protection Act, available at: https://www.pinsentmasons.com/out-law/guides/ip-addresses-and-the-data-protection-act.
- Prashant Iyengar, IP Addresses and Expeditious Disclosure of Identity in India, center for internet and society, paper available at: https://cis-india.org/internet-governance/resources, published on 22 August 2011.
- Working Document, Privacy on the Internet - An integrated EU Approach to, On-line Data Protection, Adopted on 21st November 2000.

المحتوى