مجلة جامعة سبها للعلوم البحتة والتطبيقية
Sebha University Journal of Pure & Applied Sciences
Journal homepage: www.sebhau.edu.ly/journal/index.php/jopas

استباحة خصوصية بيانات المستخدم على الانترنت ومدى وعي المستخدمين بها في ليبيا

بلعيد الدوكالي* إبراهيم البوراصي
جامعة طرابلس، ليبيا

الملخص

تتعرض هذه الدراسة لخصوصية بيانات المستخدم على الانترنت والتي باتت من المشاكل الكبرى في عالم الرقميات، حيث يتم تداول وتبادل بيانات المستخدمين على الانترنت بعلمهم وبدون علمهم من قبل شركات كبرى تهتم بهذه البيانات لاستخدمها في عمليات الدعاية والتسويق والدراسات الإحصائية، وتتبع سلوك المستخدمين. هذا ما أدى إلى زيادة الاهتمام بالنقاش حول التأثير المجتمعي للتكنولوجيا، والمخاطر التي تهدد خصوصية مستخدم الانترنت. انتظمت هذه الدراسة في مسارين، الأول هو تتبع ثلاثة مواقع شهيرة على الانترنت لمراقبة وتحديد ما تقوم به هذه المواقع من تتبع للمستخدمين وتبادل لبياناتهم وما يمثله هذا من انتهاك لخصوصية رواد تلك المواقع. أما المسار الثاني فهو - استبيانة تستهدف المستخدمين بشكل عام في ليبيا لمعرفة مدى وعيهم بتلك المخاطر. ثم خلصت هذه الدراسة إلى أن المواقع الثلاثة تقوم بتتبع بيانات المستخدمين وتبادلها مع مواقع أخرى، وأن عدداً كبيراً من أفراد عينة الدراسة لا يهتمون أو ليس لديهم وعي بالمخاطر التي تحيط بهم.

الكلمات المفتاحية:

الإنترنت، الدعاية والإعلان، التجارة الإلكترونية، أمن البيانات، خصوصية المستخدمين.

Internet user privacy violation, and measuring the extent of Libyan users' awareness.

*Baleid Aldoukali, Ebrahem Elburase

University of Tripoli, Libya

ABSTRACT

This study is exposed to the privacy of user data on the Internet, which has become one of the major problems in the digital world, where users' data is sold or exchanged on the Internet with their knowledge and without their knowledge by major companies interested in this data to use it in advertising, marketing, studies , statistics, and tracking users' behavior, this led to increased interest in the discussion about the societal impact of technology and the risks faces the privacy of Internet users. This study targeted three famous sites on the Internet to determine what these sites do in terms of tracking users and exchanging their data, and what this represents in violation of the privacy of the visitors of those sites. In addition to the above, a questionnaire has been prepared targeting Internet users to determine their awareness of these risks. The study concluded that the three sites track users' data and exchange it with other sites, and a large number of the study sample do not care or have no awareness of the dangers that surround them.

Keywords:

electronic commerce, data security, Internet, media and announcement, user privacy.

المقدمة

بالرغم من التطور الكبير في التكنولوجيا واتساع الرقعة الجغرافية لمستخدمي الانترنت لما له من فوائد كبرى في تبادل المعلومات والتعليم والاقتصاد والتسويق الالكتروني وغيرها، إلا أن هذا التطور له جانب آخر غير إيجابي وهو المتعلق بتداول وتتبع بيانات المستخدمين على الانترنت، بحيث بات من الصعب على المستخدمين - سواء أكانوا أفرادا أم مؤسسات- إخفاء بياناتهم وحجب المعلومات المتعلقة بأنشطتهم على الانترنت [1] وهذا ينطوي على عدة مخاطر تتمثل في فهم سلوك المستخدمين ورسم صورة واضحة لاتجاهاتهم خاصةً أثناء عمليات التسوق الالكتروني ، لتتمكن الجهات المعنية من إرسال مواد ترويجية لمنتجات معينة، بالإضافة إلى ذلك ، فإن المواد أو الملفات التي يقوم بتحميلها المستخدم تلقى اهتماما من قبل صائدي البيانات، ويذكر أ. البقلي [2] أن تجميع البيانات الشخصية لمستخدمي الانترنت من شأنه أن يوفر فرص الوصول إلى البيانات عن طريق التحايل أو بشكل غير مأذون به ، وهذا يفتح المجال واسعاً لإساءة استخدامها أو توجيهها بشكل خاطئ. حدد A.Jain *et al* [3] 9 طرق يمكن من خلالها الحصول على البيانات، كان أهمها سرقة البيانات عبر الإنترنت حيث بلغت 91.6% في 2020مقارنة ببقية الطرق التي منها ضياع جهاز الكمبيوتر أو النقال أو ضياع البيانات بطرق مختلفة.

يعتمد الكثير من المهتمين بجمع بيانات المستخدمين على طرق وحيل تقنية

*Corresponding author:
E-mail addresses: b.aldoukali@uot.edu.ly, (Second author) eb.elburase@uot.edu.ly
Article History: Received 00 December 00 - Received in revised form 00 January 00 - Accepted 00 February 00

وأدوات برمجية لالتقاط البيانات التي يتركها المتصفحون أثناء تصفحهم لمواقع الانترنت ، فالعديد من المواقع الكبرى مثل مواقع التسوق الالكتروني والمواقع الإخبارية تنتج عدداً كبيراً من ملفات تعريف الارتباط (الكوكيز Cookies) والتي من خلالها تستطيع تسجيل بيانات المستخدم واستخدامها في معرفة ميوله واتجاهاته ، و بالإضافة إلى ما ذكر ، هناك العديد من المواقع تطلب البريد الالكتروني للمتصفحين وتقوم بوضعها في قوائم تسمى قوائم البريد الالكتروني(Mail Lists) الغرض منها إرسال مواد ترويجية أو تحديثات تخص تلك المواقع ، وبالرغم من أن هذه الطريقة لا ضرر فيها ظاهرياً ، إلا أنها تكون عرضةً للتبادل أو البيع لجهاتٍ أخرى مهتمة ببيانات المستخدمين، وهذا ما أوردوه J. Issak and J. Hannah [4] ،حيث ذكروا أن فيسبوك قامت بمنح وصولاً غير مقيد وغير مصرح به إلى معلومات التعريف الشخصية (PII) لأكثر من 87مليون مستخدم إلى شركة Cambridge Analyticوهي شركة متخصصة في تحليل البيانات، هذه الشركة يمكن اعتبارها طرفاً ثالثاً ،Third-Partyلأنها لا تصل إلى بيانات المستخدم عن طريق جهازه مباشرة، وهذه الحادثة بينت أن فيسبوك انتهكت مرسوم الموافقة لعام 2011 مما عرضها للمساءلة من قبل لجنة التجارة الفيدرالية (FTC).

مشكلة الدراسة:

إن توسع العالم الرقمي بشكل كبير واعتماده على الإنترنت في نقل وتبادل المعلومات، فتح المجال للحصول على البيانات الشخصية للمستخدمين، فعندما تستخدم الإنترنت، فإنك تترك سجلاً للمواقع التي تزورها، جنبًا إلى جنب مع كل شيء تنقر عليه. لتتبع هذه المعلومات، تقوم العديد من مواقع الانترنت بحفظ جزء صغير من البيانات أو تضمين كائنات غير مرئية أو استخدام حسابات المستخدمين وتكوين الأجهزة، بحيث تتمكن هذه المواقع من الحصول على بيانات التصفح الخاصة بك، لتستفيد منها في معرفة اتجاهات المستخدمين ومن ثم مساعدتها في الاختيار الأفضل للمنتجات أو المواد التي يمكن ترويجها، ولكن في بعض الأحيان يؤدي الحصول على هذه البيانات إلى إساءة استخدامها ومعالجتها وتبادلها بطرق غير مشروعة، وهذا بدوره يؤدي إلى انتهاك الخصوصية الشخصية.

الإطار النظري:

إن مشكلة خصوصية المستخدم في العالم الرقمي والوصول غير المشروع لبياناته، أدى إلى اهتمام ذوي العلاقة بهذه المشكلة ومحاولة دارستها من كل جوانبها وإيجاد الحلول الناجعة لها، ولهذا وجب عرض بعض المفاهيم والتعريفات المهمة التي يتم تداولها أثناء البحث عن حلول لهذه المشكلة.

أولا: البيانات الشخصية والخصوصية

يقصد بالبيانات الشخصية، هي تلك البيانات التي تميز الشخص عن غيره كالاسم واللقب والعمر والديانة، بالإضافة إلى معرفات أخرى كالبطاقة الشخصية أو جواز السفر، ويضاف إليه في العالم الرقمي البريد الالكتروني واسم المستخدم وكلمة المرور وغيرها. تعتبر هذه البيانات خاصةً بالشخص الذي يحملها ولا يجوز استخدامها من قبل غيره إلا بإذن صاحبها، وإلا فإنه يعتبر تعدياً على الخصوصية الشخصية.

إن مفهوم خصوصية البيانات الشخصية أثير منذ زمن بعيد، حيث عرفه آلان ويلسون في مؤلفه (الخصوصية والحرية Privacy and Freedom) بأنه "*حق الأشخاص في تحديد متى وكيف تصل المعلومات الخاصة عنهم للآخرين*"[5]، ومن ثم، فإن هذا الحق يخص صاحب البيانات وحده وهو حر في إعطاء هذه البيانات أو منعها. إن الغالبية من مستخدمي الانترنت يميلون لإعطاء بياناتهم الشخصية إذا كانت هناك ثقة أو شفافية في التعامل معهم وأشاروا A. Oulasvirta *et al* [6] أنها تضحية طوعية.

ثانيا: التجارة الإلكترونية

إن أساليب التجارة تتطور بمرور الزمن، فمن بيع مباشر في محلات صغيرة، توسعت إلى مؤسسات وفروع، وإلى شركات دولية، ومع تزايد العمليات التجارية وظهور التقنية وتطورها، ظهرت أساليب جديدة في العمليات التجارية، أهمها استغلال شبكة الإنترنت في تسويق المنتجات التجارية بجميع أنواعها، والتي أتاحت تفاعلا وتواصلا أكبر بين التجار والعملاء، وفكت الارتباط بالزمان والمكان في التعامل. ومع تزايد رواد الانترنت وتضخم التجارة الإلكترونية وتوسعها فإن التجار والمسوقين بحاجة إلى الوصول إلى المستهلك داخل هذه الشبكة العنكبوتية، ولذلك عمدوا إلى إتباع أسلوب الإعلانات التجارية عبر الإنترنت للإعلان عن منتجاتهم، ليس في المواقع الخاصة بهم فحسب، بل بتتبع المستخدمين في المواقع غير التجارية التي يرتادونها، هذا الأسلوب زاد من أرباح التجار وظهور تجارة الإعلانات التي تذر أرباحاً ضخمة. يذكر م.مهنى [1] أن الإنفاق العالمي على الإعلانات بلغ 389 مليار دولار عام 2021، وهذا الرقم في تزايد مستمر بسبب الإقبال الشديد على التسوق عبر الإنترنت.

ثالثاً: أساليب الوصول للمستخدم وتقنياته.

إن تسويق المنتجات والإعلان عنها عبر الانترنت يتطلب طرقاً وتقنيات متنوعة للوصول للعميل بأقل تكلفة وأسرع وقت من أهمها:

1. **ملفات تعريف الارتباط Cookies**: وهي عبارة عن ملفات نصية ذات حجم صغير يتم تكوينها داخل جهاز المستخدم بمجرد زيارته لموقع الإنترنت، تحتوي على عددٍ من البيانات التي تخص المستخدم، ويتم استغلالها في معرفة ميوله واتجاهاته، ومن تم إرسال الإعلانات المناسبة، هذه الملفات تكون عرضةً للوصول إليها من قبل المواقع الأخرى التي يتم زيارتها، وتبادلها أو تحليلها وتعريض الخصوصية للانتهاك [7].
2. **البريد الإلكتروني:** تطلب مواقع التسوق الالكتروني التسجيل والاشتراك بالبريد الإلكتروني لضمان إرسال بيانات المنتجات وتحديثات الأسعار والإخطار بوصول المنتجات الجديدة. بعض هذه المواقع تستخدم أساليب ملتوية الغرض منها الحصول بشكل غير قانوني على قوائم البريد الإلكتروني الخاصة بأصدقاء المستخدم ومن تم إعادة إرسال المواد الإعلانية إليهم.
3. **شبكات التواصل الاجتماعي:** يتم من خلال هذه المواقع والتي من أشهرها Facebook إرسال عدد كبير من الإعلانات التجارية لرواد شبكات التواصل الاجتماعي. تهدف مواقع الإنترنت، وبخاصة مواقع التواصل الاجتماعي، إلى تحقيق غرضٍ تجاريٍ محدد هو تسويق البيانات ذات الطابع الشخصي لمستخدميها، من أجل إدارة الحملات الإعلانية التي تعد مورداً هاماً من مواردها، بل إن هذه الإعلانات تعد المصدر الأول لأرباح هذه المواقع [8].من ناحية أخرى، فإن مستخدمي شبكات التواصل الاجتماعي يتعرضون لانتهاك الخصوصية من قبل

مستخدمين آخرين، حيث يشير ع. الطيب [9] لازدياد ظاهرة استغلال مواقع التواصل الاجتماعي في انتهاك الخصوصية للدرجة التي أصبحت فيها الظاهرة تشكل خطراً إجرامياً مهدداً للسلامة المجتمعية.

4. **برامج الدعاية (Ad Ware) وبرامج التجسس (Spy Ware):** يتم إدخال هذه البرامج خفية في جهاز المستخدم بطرق عدة كتضمينها مع برنامج آخر غير ضار، وتهتم هذه البرامج بجمع بيانات المستخدم من بقايا ملفات تعريف الارتباط المتروكة في جهاز المستخدم أو عن طريق البحث داخل الجهاز عن أي معلومة يمكن الاستفادة منها وإرسالها إلى مواقع التسوق أو شركات تحليل البيانات لاستخدامها في التسويق أو أي أغراض أخرى.
5. **أدوات ومو اقع جمع البيانات وتحليلها:** بعض الشركات تقدم خدمة لمواقع التسوق ومواقع الأخبار والمواقع المهتمة ببيانات المستخدم، هذه الخدمة تتكفل الشركات بتتبع كل تحركات المستخدمين داخل موقع الإنترنت وتسجيل سلوكه والروابط التي يتبعها داخل الموقع، بل وحتى نقرات الماوس وما يكتبه، بالإضافة إلى تسجيلات فيديو لحركة المستخدم داخل الموقع، ويستفاد من هذه الإجراءات في تحليل سلوك رواد الموقع ومن تم اتخاذ القرارات المناسبة حسب طبيعة كل موقع. ومن أشهر تلك المواقع موقع Hotjar وهو حل متكامل لتحليلات مواقع الويب يتضمن خرائط حرارية (Heatmap) لسلوك المستخدم وتسجيلات الجلسة مع تتبع الماوس ومسارات التحويل واستطلاعات الرأي والاستطلاعات الكاملة وتسجيل نقرات الماوس للمستخدم.

ثالثاً: لو ائح حماية الخصوصية وقو انينها.

سنت العديد من الدول قوانين ولوائح لحماية خصوصية مستخدمي الانترنت، لأن هذه الخصوصية تعترضها عدة مخاطر في العالم الرقمي، فهي عرضة للانتهاك والتبادل بشكل غير قانوني، أهمها الإعلان العالمي لحقوق الإنسان الذي صدر عن الجمعية العامة للأمم المتحدة عام 1948، والذي جاء في نص مادته رقم 12 "*لا يجوز تعريض أحد لتدخل تعسفي في خصوصيته أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته. لكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات*"[2]. وقد تنوعت القوانين واللوائح على اختلاف مستوياتها ، فهناك قوانين على مستوى الولايات كما في ولاية كاليفورنيا في الولايات المتحدة حيث أقرت قانوناً سمي قانون خصوصية المستهلك في كاليفورنيا (California Consumer Privacy Act CCPA)، وهناك قوانين على مستوى الدولة مثل LGPD في البرازيل و PDPA في سنغافورة، أما على مستوى الدول العربية فقد نجحت تونس في سن القانون رقم 63 لسنة 2004حول الخصوصية وحماية البيانات الشخصية ، ووضعت إمارة دبي تشريعاً لحماية البيانات الشخصية خاص بمركز دبي المالي [10] ، وهناك قوانين على مستوى عدة دول كما هو الحال في دول الإتحاد الأوروبي GDPR.

- **اللائحة العامة لحماية البيانات أوGDPR**

اتفقت دول الإتحاد الأوروبي على لائحة تسمى (اللائحة العامة لحماية البيانات General Data Protection Regulation) أو GDPR رقم 2016/679 بتاريخ 5 أبريل 2016 [11] ،هذه اللائحة تنطبق على كل مواقع الانترنت التي يتم استضافتها داخل مزودات خدمة الانترنت في نطاق دول الاتحاد الأوروبي ، وهو مصمم لمواءمة قوانين خصوصية البيانات من أجل حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات ، حيث أشارت هذه اللائحة أنه في حال السماح لأي من الطرفين ("الطرف المتلقي") أو وكلائه أو مقاوليه أو موظفيه بالوصول إلى البيانات الشخصية التي يحتفظ بها الطرف الآخر لأي سبب من الأسباب أو تم تزويدها أو توفيرها بأي طريقة أخرى من قبل الطرف الآخر لأي غرض من الأغراض ، يجب على الطرف المتلقي أو وكلائه أو مقاوليه أو موظفيه، الالتزام بالآتي:

1. استخدام و / أو الاحتفاظ بهذه البيانات الشخصية فقط للأغراض وبالطريقة التي يوجهها الطرف الآخر ولا يجوز لهم تعديل أو تغيير محتويات هذه البيانات الشخصية ما لم يأذن بها الطرف الآخر كتابيًا ويتعين اتخاذ جميع الخطوات اللازمة لحماية هذه البيانات الشخصية.
2. الامتثال لجميع النواحي للائحة وكذلك القانون المحلي المعمول به ولا يجوز أو يسمح بأي شيء قد يعرض للخطر أو يتعارض مع شروط إخطار الطرف الآخر بموجب اللائحة أو القانون المحلي المعمول به.
3. تعويض الطرف الآخر عن جميع المسؤوليات والأضرار والتكاليف والمطالبات والمصروفات التي قد يتكبدها بسبب أي تقصير بموجب هذا البند أو أي خرق للائحة أو القانون المحلي الساري المنسوب إلى أو الناجم، بشكل مباشر أو غير مباشر، عن طريق الطرف المتلقي أو موظفيه أو وكلائه أو مقاوليه، بما في ذلك على سبيل المثال لا الحصر، عدم منع الكشف عن ذلك بما يتعارض مع اللائحة أو القانون المحلي المعمول به.

- **قانون ملفات تعريف الارتباطCookies Law**

هو جزء من تشريع الخصوصية الذي يتطلب من مواقع الإنترنت الحصول على موافقة من الزوار لتخزين أو استرداد أي معلومات على جهاز كمبيوتر أو هاتف ذكي أو جهاز لوحي. تم تصميمه لحماية الخصوصية عبر الإنترنت، من خلال توعية المستخدمين بكيفية جمع المعلومات المتعلقة بهم واستخدامها عبر الإنترنت، ومنحهم خيار السماح بذلك أم لا، ومن تم حصولهم على مزيد من التحكم في خصوصيتهم عبر الإنترنت.[12]. إن القانون طالب مواقع الانترنت بإبلاغ الزوار والحصول على موافقتهم على استخدام ملفات تعريف الارتباط داخل أجهزتهم، وهذا ما يتم ملاحظته أثناء الدخول للموقع، حيث يظهر شريط عريض ينبه المستخدم بإن الموقع سوف يستخدم ملفات تعريف الارتباط، ويمنحه إمكانية الموافقة من عدمها. وبالرغم من التزام عدداً كبيراً من المواقع بهذا القانون، إلا أن عدد كبير من رواد الإنترنت لا يستخدمون هذه الخاصية بشكل فعال، وهذا ما ذكروه M. Rudolf *et al* [13] في نتائج بحثهم.

رابعا: تتبع المستخدمين من قبل متتبعي الطرف الثالث Third-Party Trackers

عندما يقوم المستخدم بزيارة موقع ما فإن هذا الموقع يعتبر طرفاً أول، لأنه يقوم بتقديم الخدمة مباشرة والتفاعل مع المستخدم الذي هو الطرف الثاني، ولكن عدد كبير من المستخدمين لا يعلمون أن هناك طرفاً ثالثاً يقوم بتجميع بياناتهم، حيث يشير تتبع الطرف الثالث إلى التتبع الذي تقوم به مواقع الإنترنت التي لا يتنقل المستخدم إليها أبدًا بشكل صريح. يدرك العديد من مستخدمي الإنترنت بشكل غامض أنه قد يتم جمع معلوماتهم عبر الإنترنت. ومع ذلك، يشير S.Mittal [14] إلى وجود معرفة قليلة نسبيًا بتتبع الطرف

الثالث ومخاطر الخصوصية المرتبطة به. تستخدم شركات الطرف الثالث ملفات تعريف الارتباط عبر المواقع لجمع معلومات حول مواقع الانترنت التي تزورها وإرسالها إلى شركات أخرى، غالبًا لأغراض الدعاية. وهذا يظهر جلياً عندما ترى أن إعلانًا ما يتابعك أثناء التصفح، فهذا نتيجة للتتبع عبر المواقع إذا كان المتتبع نفسه موجودًا على مواقع متعددة. من أشهر شركات تتبع الطرف الثالث DoubleClick وAmazon Ad System و Cambridge Analytica. ويمكن أيضا إنشاء ملف تعريف أكثر اكتمالاً بمرور الوقت ، هذا الملف أو المعرف الخاص بالمستخدم لا يستوجب الحصول على ملفات تعريف الارتباط ، فهناك طرق أخرى يمكن من خلالها تكوين معرف للمستخدم ، كأن يتم تجميع معلومات عن جهاز المستخدم مثل معرفة نسخة المتصفح ونسخة الويندوز وقائمة بالخطوط الموجودة داخل الجهاز وبعض البيانات الأخرى ، ومنها يمكن تكوين معرف فريد للجهاز يطلق عليه Fingerprint من خلاله يمكن تتبع جهاز المستخدم ومعرفة أي من المواقع التي قام بزيارتها ، يذكر A. Narayanan and D. Reisman [15] أن متتبعي الطرف الثالث يستخدمون تكتيكات أكثر خبثاً والتواء بحيث يصعب على المستخدم حماية نفسه من التتبع.

الدراسات السابقة:

ظهرت العديد من الدراسات التي تتعرض لمشكلة خصوصية المستخدمين على الإنترنت وأبرزت العديد من المخاطر التي كانت مخفية عن المستخدمين، من هذه الدراسات:

- **بحث محمود منى (2022)** [1]: ويهدف هذا البحث إلى تحديد اتجاهات الجمهور نحو تأثير استخدام التسوق الإلكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة على الخصوصية في العصر الرقمي، حيث استهدف البحث عينة بلغت 392 شابا من الجامعات المصرية على أساس أنهم الشريحة الأنشط على شبكة الإنترنت. أشارت النتائج إلى معرفة متوسطة بتطبيقات التكنولوجيا الحديثة بلغ 58%، وأن 89% من أفراد العينة أظهروا مستويات مختلفة من القلق على خصوصية بياناتهم على الإنترنت .وعزاه إلى عدم وجود تشريعات وقوانين كافية لحماية الخصوصية الرقمية. كما اختبر عدداً من الفرضيات وأظهر أن ارتفاع مستوى معرفة المستخدمين بالتكنولوجيا في مجال التسوق الإلكتروني يساهم في زيادة وعيهم بالتهديدات التي تتعرض لها خصوصيتهم.

- **بحث منى الموسوي وجان فضل الله (2013)**[16]يسلط الضوء على الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها وكيفية الحماية. في هذا البحث صمم استبيان من أجل تقصي سلوك المستهلكين تجاه الخصوصية المعلوماتية ومخاطر التقنيات الحديثة عليها لتحقيق الأهداف المرجوة من البحث، وقد شمل الاستبيان407 عينة دراسة وزعت عشوائيا على مجموعة من مواطني محافظة بغداد. خلص البحث إلى أن غياب سياسة حماية الخصوصية المعلوماتية أو عدم تطبيقها في العراق ولَّد عدم ثقة كافية بين المواطن ومؤسسات الدولة التي يزودونهم بمعلوماتهم الشخصية في الوقت الراهن، بالإضافة إلى عدم وجود قوانين أو تشريعات في العراق تحمي معلومات المواطن الشخصية من الانتهاك من قبل الآخرين.

وأخيرا فقد أوصى الباحثون بـ:

1. ضرورة قيام المسئولين بتشريع قوانين تحمي سرية الخصوصية المعلوماتية في العراق.
2. ضرورة تلقي مستخدمي الانترنت والمواطنين بشكل عام دورات تثقيفية حول حماية خصوصيتهم المعلوماتية.
3. إقامة الندوات والدورات والمؤتمرات حول هذا الموضوع من حيث مناقشة أبعاده وتأثيره على المجتمع العراقي.

- في دراسة**Xuehui Hu , Nishanth Sastry (2020)** [17]،تم النظر في تتبع وترابط الطرف الثالث، باستخدام عينات مستخدمين من المملكة المتحدة والصين الذين قاموا بزيارة أفضل 500 موقع على الويب من Alexa، والاعتماد على سجلات التصفح الحقيقية قسمت العينات إلى مجموعتين من المستخدمين: الأولى فئة مختارة بعناية من 15مستخدمًا،9من المملكة المتحدة و6 من الصين، والأخرى مجموعة من 124 مستخدمًا من 25دولة مختلفة في العالم اختارت التبرع بالبيانات لمشروع هذه الدراسة. تم في هذه الدراسة تقديم مقياس جديد سمي (عامل التشابكTangle Factor) لقياس مدى تتبع الطرف الثالث لبيانات المستخدم، باستخدام هذا المقياس، تبين أن مستخدمو المواقع الصينية أقل تعقبًا من المستخدمين للمواقع في المملكة المتحدة، ويرجع ذلك على الأرجح إلى الحظر التلقائي لأجهزة التتبع الرئيسية مثل Googleو Facebook من جدار الحماية العظيم في الصين. أيضًا تم استخدام مقياس عامل التشابك للمقارنة بين أدوات حظر الإعلانات وأظهر أن أداة uBlock تعمل بشكل أفضل من غيرها مثل ghostery و Ad blocker plus وad guard. كما أظهر البحث أن الحماية الافتراضية التي يوفرها Firefox أفضل من تلك التي يوفرها Google Chrome.

- **بحث Ankit Jain, et al (2021)** [3]: مع التكنولوجيا سريعة النمو، انتشرت شبكات التواصل الاجتماعي عبر الإنترنت (OSN) بشكل كبير على مدى السنوات القليلة الماضية. سبب هذا الانتشار هو قدرة OSN على توفير منصة للمستخدمين للتواصل مع عائلاتهم وأصدقائهم وزملائهم. وتنتشر المعلومات التي تتم مشاركتها في الشبكات الاجتماعية والوسائط بسرعة كبيرة، وبشكل شبه فوري مما يجعل الحصول على المعلومات أمرًا جذابًا للمخترقين. ولهذا قام الباحثون بدراسة عن السرية والضمان من OSNs من مختلف الجوانب، وخلصوا إلى أن هناك العديد من مشكلات الأمان والخصوصية المتعلقة بالمعلومات المشتركة للمستخدم، خاصةً عندما يقوم المستخدم بتحميل المحتوى الشخصي مثل الصور ومقاطع الفيديو والتسجيلات الصوتية. بحيث يمكن للمهاجم استخدام المعلومات المشتركة بشكل ضار ولأغراض غير مشروعة، وتكون المخاطر أعلى إذا تم استهداف الأطفال. لمعالجة هذه القضايا، قدم الباحثون مراجعة شاملة لتهديدات الأمان والخصوصية المختلفة والحلول الحالية التي يمكن أن توفر الأمان لمستخدمي الشبكات الاجتماعية. وناقشوا أيضًا الهجمات المختلفة على تطبيقات الويب من خلال شبكات التواصل الاجتماعي. بالإضافة إلى ما سبق، ناقشوا من خلال استطلاع القضايا المفتوحة والتحديات وإرشادات الأمان ذات الصلة لتحقيق الثقة في الشبكات الاجتماعية عبر الإنترنت.

- **بحث Julia Erap, et al (2005)**[18]نتجت عنه أداة مسح تحتوي على 36 عنصر قياس تتعلق ببيانات الخصوصية الخاصة بالاستخدام المستقبلي من

قبل الباحثين والمديرين التنظيميين. المساهمة الرئيسية لهذه الدراسة هي إظهار الفجوة بين ما يراه المستخدم وما تؤكده سياسات خصوصية مواقع الويب. وقد أوصى الباحثون بأن تكون المؤسسات على يقين من تضمين عبارات تعالج مخاوف المستخدمين. على وجه التحديد، يجب أن تكون المؤسسات على يقين من تضمين العبارات التي تتناول:

1. كيفية مشاركة بيانات المستخدمين أو تبادلها أو بيعها للآخرين (على سبيل المثال، "يجوز لنا مشاركة معلومات ملف تعريف حسابك مع شركائنا في العمل والشركات الفرعية لتحليل التسويق والجهود التعاونية الأخرى بين مؤسساتنا. ") ؛
2. إبلاغ المستخدمين بكيفية استخدام معلوماتهم الحساسة قبل تقديمها (على سبيل المثال، "إذا اخترت تزويدنا بعنوان بريدك الإلكتروني، نحتفظ بالحق في استخدامه للاتصال بك بخصوص التغييرات إلى موقعنا الإلكتروني، ولتزويدك بأحدث المستجدات ومعلومات عن عروض منتجاتنا وخدماتنا. ") .
3. كيفية تخزين بيانات المستخدم وحفظها بشكل آمن (على سبيل المثال، "يتم تشفير جميع المعلومات التي يتم جمعها عبر هذا الموقع باستخدام SSL خلال عملية الجمع. ثم يتم تخزينه محليًا أوفي منشأة خارج الموقع، حيث يقتصر الوصول إلى كلهما على الموظفين الذين يحتاجون إلى الوصول إلى هذه المعلومات، والوصول يقتصر فقط على تلك الضرورية والمحددة لمهمة معينة.").
4. يجب أن تبذل المنظمات جهودًا متضافرة لتضمين عبارات مشابهة للأمثلة المذكورة للتأكيد بأنها تناولت العناصر ذات الأهمية الكبرى لمستخدميها وهي: البيانات، نقل البيانات، الإشعار والوعي، وتخزين البيانات.

منهجية الدراسة:

إن موضوع خصوصية بيانات المستخدم على الانترنت يستوجب دراسة الحالة من جانبين، الجانب الأول هو المواقع التي تقدم الخدمة للمستخدمين باعتبارها طرفاً أول وما يدور حولها من جدل بخصوص المحافظة على بيانات المستخدمين، أما الجانب الآخر فهو المستخدم نفسه باعتباره المستفيد من الخدمة التي تقدمها مواقع الانترنت، وما يزود به المواقع من بيانات شخصية. بالنسبة للجانب الأول، وهو مواقع الانترنت تم استخدام أدوات برمجية لتحليل ملفات تعريف الارتباط لتلك المواقع وتحديد سلوكها في تتبع بيانات المستخدم وعلاقتها بمواقع (الطرف الثالث). أما الجانب الثاني وهو جانب المستخدم فقد تم اعتماد المنهج الوصفي التحليلي في تحديد مدى وعي المستخدمين بموضوع الخصوصية.

مجتمع الدارسة:

<u>أولا: الجانب الأول (مو اقع الإنترنت)</u>

تم اختيار ثلاثة مواقع على الإنترنت وهي:

1. موقع قناة الجزيرة الإخبارية www.aljazeera.net.
2. موقع أمازون للتسوق الإلكتروني www.amazon.com.
3. وموقع (علي بابا) للتسوق الإلكتروني www.alibaba.com.

وهي مواقع تتميز بعدد زوار كبير جداً.

<u>ثانيا: الجانب الثاني (المستخدمين)</u>

تم اختيار عينة عشوائية من مستخدمي الانترنت في ليبيا بلغت 200 مستخدم لمعرفة مدى وعيهم بالمخاطر التي تواجههم من ناحية الخصوصية على الإنترنت.

أدوات الدراسة:

إن دراسة وتحليل سلوك مواقع الانترنت ومعرفة ما تقوم به إزاء بيانات المستخدم، يستوجب استعمال أدوات برمجية واستغلال ما تقدمه متصفحات الإنترنت من خدمات في هذا المجال، ولهذا، فقد تم استخدام أداة برمجية تسمى LightBeam وظيفتها تتبع ومراقبة ملفات تعريف الارتباط للمواقع النشطة التي يعرضها المستخدم في متصفح الإنترنت الخاص به، أضف إلى ذلك فإن متصفحي Firefox وGoogle Chrome يوفران إمكانية معرفة ملفات الارتباط التي يتم تداولها من قبل مواقع الإنترنت. وأخيراً، وبالاستعانة بموقع www.privacyscore.org أمكن الحصول على نتائج تحليل أكثر شمولية.

أما من جانب المستخدم فقد تم تصميم استبيان مغلق محدد بإجابة نعم أو لا، يحتوي على بيانات شخصية وعلى عدد من الأسئلة لمعرفة مدى وعي المستخدمين بموضوع الخصوصية. تم تصميم نسخ إلكترونية عن طريق Google Forms ونشرها في عدد من صفحات التواصل الاجتماعي الليبية، وفيما يلي مجموعة من الخطوات المستخدمة في تحميل البيانات:

1. تم تجهيز الاستبيان اعتمادا على دراسة ن. جبر *وآخرون* [19] مع إجراء بعض التعديلات وعرضها على بعض المختصين ليتناسب الاستبيان مع طبيعة هذه الدراسة.
2. قسم الاستبيان إلى محورين: الأول خاص بمدى وعي المستخدم بخصوصية بياناته ويحتوي على (5) أسئلة، والمحور الثاني خاص بمعرفة المستخدم بموضوع جمع وتخزين بياناته وتداولها بين المواقع ويحتوي على (7) أسئلة.
3. تم استخدام الإحصائيات الوصفية (النسبة المئوية، التكرارات) للتعرف على الصفات الشخصية لمفردات الدراسة وتحديد استجابات أفرادها تجاه عبارات المحاور الرئيسية التي تتضمنها أداة الدراسة.
4. تم الحصول على النتائج من خلال برنامج التحليل الإحصائي SPSS النسخة 20.0 لحساب التكرارات والمتوسط الحسابي والنسب المئوية.

نتائج الدراسة:

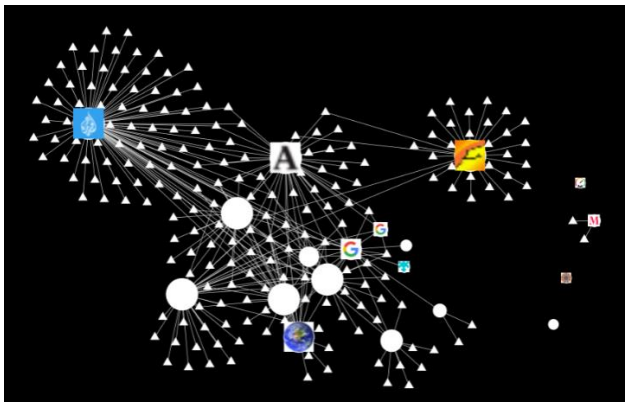
1- الجانب الأول (مو اقع الإنترنت).

<u>نتائج الفحص بأداة LightBeam</u>

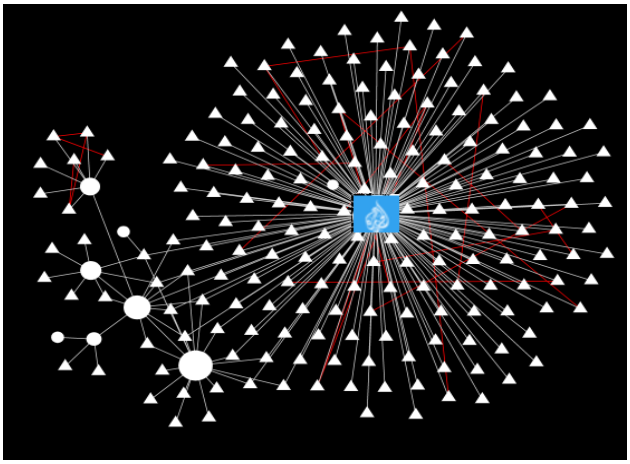
بعد استخدام LiteBeam للمواقع الثلاثة الذي تم ذكرها سابقاً، أظهرت الأداة جميع مواقع الطرف الثالث التي تتعامل معها المواقع الثلاثة المذكورة، وبالرغم من أن العديد من تلك المواقع يتم من خلالها استيراد بعض السكربتات البرمجية المهمة لتشغيل المواقع قيد الدراسة، إلا أن هناك العديد من تلك السكربتات وملفات الارتباط الأخرى تقوم

بالحصول على بيانات المستخدمين وإرسالها إلى الطرف الثالث. والشكل رقم (1) يبين تخطيط رسومي للمواقع الثلاثة وارتباطها بمواقع الطرف الثالث، حيث تظهر الدوائر البيضاء المواقع التي زرناها من ضمنها مواقع الجزيرة وأمازون وعلي بابا، والمثلثات البيضاء تشير إلى مواقع الطرف الثالث التي تتصل بها.

أما الشكل رقم (2) فهو لموقع قناة الجزيرة الإخبارية بشكل أكثر تفصيلاً، حيث يظهر عددا كبيرا من مواقع الطرف الثالث المرتبطة بموقع الجزيرة الإخبارية، وتشير الخطوط الحمراء إلى ارتباط مجموعة من مواقع الطرف الثالث بحيث تتم مزامنة ملفات تعريف الارتباط التي تم الحصول عليها من الموقع المذكور. وكما ذكرنا سابقا، فإن المواقع الموجودة في الشكل (2) ليست كلها لها أغراض دعائية أو غير قانونية، فهناك العديد منها يستخدمها موقع الجزيرة الإخبارية لاستيراد سكربتات وملفات تنسيقية CSS لإظهار الموقع بشكل منسق.



الشكل 1. رسم تخطيطي يظهر المو اقع الثلاثة وارتباطها بالطرف الثالث



الشكل 2ارتباط موقع قناة الجزيرة الإخبارية بالطرف الثالث

نتائج الفحص عن طريق Privacyscore.org

بعد فحص المواقع الثلاثة عن طريق privacyscore.org، تم الحصول على 48 معيار فحص مختلف، تم أخذ 8 معايير لها علاقة بخصوصية بيانات المستخدمين وتم تفريغها في الجدول رقم (1)، وفيما يلي شرح مبسط للمعايير الثمانية:

1. **عدد مو اقع الطرف الثالث المضمنة:** العديد من المواقع تستخدم خدمات وملفات من مواقع الطرف الثالث وذلك لتحسين مظهر وأداء الموقع، ولكن هذه الخدمات لها محاذير على مستوى خصوصية زوار الموقع.
2. **مو اقع الطرف الثالث (تتبع - دعائية):** هذا المعيار يظهر عدد مواقع الطرف الثالث المعروفة بأنها تقوم بتتبع بيانات المستخدم أو لها خدمات دعاية عبر المواقع.
3. **عدد ملفات تعريف الارتباطcookies:** يشير إلى عدد ملفات تعريف الارتباط التي يخزنها الموقع في جهاز المستخدم وهي نوعان، طويلة المدى والتي تبقى في جهاز المستخدم مدة طويلة من الزمن تصل إلى أسابيع وأخرى قصيرة المدى تدوم لدقائق.
4. **عدد ملفات تعرف الارتباط المضمنة من الطرف الثالث:** هذه الملفات المضمنة تخص مواقع الطرف الثالث المعروفة بالتتبع أو نشر الدعايات عبر المواقع.
5. **استخدام تحليلات google:** تقوم شركة غوغل بتوفير خدمات تحليل بيانات كثيرة من ضمنها الخاصة بسلوك المستخدمين، بحيث تستخدم هذه النتائج في تحسين خدمات المواقع.
6. **هل خادم الانترنت يقع ضمن نطاق الدول التي تطبق لائحة GDPR:** هذا المعيار يفحص ما إذا كان خادم الويب الذي يستضيف الموقع يقع ضمن نطاق دول الإتحاد الأوروبي التي تطبق اللائحة العامة لحماية البيانات.
7. **هل خادم البريد يقع ضمن نطاق الدول التي تطبق لائحة GDPR:** هل خوادم البريد الالكتروني الخاصة بتلك المواقع تقع ضمن نطاق دول الإتحاد الأوروبي التي تطبق اللائحة العامة لحماية البيانات.
8. **تطبيق سياسة أمن المحتوى CSP في ترويسة Http:** هل هذه المواقع تطبق سياسة أمن المحتوى (Content-Security Policy CSP) وتضمنها في ترويسة Http في صفحات الموقع، وهي مهمة للحماية من هجمات (Cross-Site Scripting XSS) والتي تستخدمها بعض مواقع الطرف الثالث الدعائية لتضمين سكربتات برمجية وظيفتها جمع بيانات المستخدم.

جدول (1) نتائج معايير فحص المو اقع الثلاثة

نوع الفحص	موقع الجزيرة الاخبارية **aljazeera.net**	موقع أمازن **amazon.com**	موقع علي بابا **alibaba.com**
عدد مواقع الطرف الثالث المضمنة	33	48	21
مواقع الطرف الثالث (تتبع - دعائية)	17 - من أشهرها a.pub.network bam-cell.nr-data.net d.pub.network geolocation.onetrust.com metrics.brightcove.com sb.scorecardresearch.com static.chartbeat.com stats.g.doubleclick.net www.google-analytics.com	40 - من أشهرها aa.agkn.com ads.samba.tv ads.stickyadstv.com.com analytics.twitter.com c1.adform.net cm.g.doubleclick.net cms.analytics.yahoo.com googleads.g.doubleclick.net pixel.advertising.com adsystem.com sb.scorecardresearch.com sec.casalemedia.com sync.search.spotxchange.com	8 - من أشهرها gcd.mmstat.com gj.mmstat.com mc.yandex.com mc.yandex.ru retcode-us-west-1.arms.aliyuncs.com s.alicdn.com stats.g.doubleclick.net www.google-analytics.com
عدد ملفات تعريف الارتباط cookies (طويلة المدى – قصيرة المدى)	6 - 6	1 - 7	14 – 15
ملفات تعرف الارتباط المضمنة من الطرف الثالث (طويلة المدى – قصيرة المدى)	2 - 3	2 - 46	5 - 10
الموقع لايستخدم تحليلات google	×	✓	×
هل خادم الانترنت يقع ضمن نطاق الدول التي تطبق لائحة GDPR	✓ هولندا	× الولايات المتحدة	✓ هولندا
هل خادم البريد يقع ضمن نطاق الدول التي تطبق لائحة GDPR	× قطر	× الولايات المتحدة	× الصين
تطبيق سياسة أمن المحتوى CSP في ترويسة Http	×	×	×
تشير علامة ✓ إلى التزام الموقع بتطبيق المعيار وعلامة × تشير إلى عدم الالتزام أو عدم وجودها في نطاق الدول التي تطبق هذا المعيار			

من خلال الجدول رقم (1) يتبين أن المواقع الثلاثة تستخدم الكثير من خدمات الطرف الثالث، ومن تم، فإن هناك فرصة لتواجد أطراف أخرى خاصة بتتبع بيانات المستخدم لاستخدامها في أغراض مختلفة قد تكون غير قانونية أحياناً، وهذا يظهر جليا في المعيار رقم (2) خصوصا في موقع أمازون الذي يحتوي على 40 من متتبعي الطرف الثالث.

المشكلة الأخرى تكمن في وجود ملفات تعريف الارتباط cookies طويلة المدى والتي تبقي في جهاز المستخدم حتى بعد إغلاق المتصفح والتي قد تبقى لأسابيع . وهذه عرضة للحصول عليها من المتتبعين ومروجي الدعايات. وهناك أيضا ملفات تعريف الارتباط التي تضمن من قبل متتبعي الطرف الثالث، ويظهر أن موقع أمازون يتضمن 46 ملف تعريف ارتباط وموقع علي بابا يحتوي على 10 ملفات.

أما بالنسبة لوجود خوادم الويب التي تستضيف المواقع ضمن نطاق دول الاتحاد الأوروبي والتي تطبق اللائحة العامة لحماية البيانات GDPR فإن موقع أمازون لا يقع من ضمن نطاق هذه اللائحة. وكذلك الحال بالنسبة لمزودات خدمة البريد الإلكتروني فإن المواقع الثلاثة لا تقع خدمات البريد الالكتروني لديها في نطاق الـ GDPR، حيث يقع الخادم الخاص بموقع الجزيرة في قطر وأمازون في أمريكا وعلي بابا في الصين. إن عدم وجود خادم الويب وخادم البريد الالكتروني في نفس النطاق يؤدي إلى إرسال ومعالجة البيانات خارج نطاق خادم الويب أي في دولة أخرى وهذا يؤدي في بعض الأحيان لتعريض هذه البيانات للخطر.

وأخيراُ، فإن تطبيق سياسة أمن المحتوى CSP للحماية من هجمات XSS يمنع إلى حد ما متتبعي الطرف الثالث غير المخولين من إرسال سكربتات برمجية للحصول على بيانات من شأنها أن تعرض خصوصية مستخدمي تلك المواقع للخطر وهذا ما لم يتوفر في المواقع الثلاثة قيد الدراسة.

الجانب الثاني (وعي المستخدم بمخاطر انتهاك الخصوصية)

تم استلام (119) عينة بخلاف المستهدف وهو 200 عينة، تم تفريغها في برنامج SPSS لحساب التكرارات والنسب المئوية لكل فقرة من فقرات الاستبيان بالإضافة إلى البيانات الشخصية لكل عينة وكانت النتائج على النحو الأتي:

أولاً: البيانات الشخصية لأفراد العينة

- **جنس العينة**: يظهر الجدول رقم (2) أن نسبة الذكور أعلى من نسبة الإناث في المشاركة في الاستبيان، حيث بلغت نسبة الذكور88% من أفراد العينة بينما 12% الباقية هي للإناث.

جدول (1) النسب والتكرارات لجنس العينة

جنس العينة	التكرار	النسبة المئوية
ذكر	14	%12
أنثى	105	%88

جدول (2) التكرارات والنسب المئوية للعمر

العمر	التكرار	النسبة المئوية
أقل من 10 سنوات	1	%1
من 10 إلى 30 سنة	14	%12
من31 إلى 50 سنة	92	%77
من 51 إلى 70	12	%10
أكثر من 70 سنة	0	%0

من خلال الجدول رقم (3) يتبين أن أعلى نسبة من رواد الإنترنت هي في الفترة من 31 إلى 50 سنة حيث بلغت 92% من أفراد عينة الدراسة وهي مرحلة النشاط والوعي لدى الإنسان.

- **عدد الساعات التي يقضيها على الإنترنت:** أغلب المستخدمين يقضون من ساعة إلى ثلاث ساعات ومن ثلاث ساعات إلى 6 ساعات على الانترنت، حيث بلغت 45% و43% على التوالي كما هو مبين في الجدول رقم (4)، وهذا يبين أن زمن تواجد المستخدمين على الانترنت هو زمن كبير، وهذا يزيد من نسبة تعرضهم للانتهاك بمختلف أشكاله.

جدول (3)عدد الساعات التي يقضيها على الانترنت

عدد الساعات	التكرار	النسبة المئوية
أقل من ساعة	7	%6
من ساعة إلى 3 ساعات	45	%38
من 3 ساعات إلى 6 ساعات	42	%35
أكثر من 6 ساعات	25	%21

ثانياً: مدى وعي المستخدم بخصوصية بياناته:

- **هل تعرف ماذا تعني سياسة الخصوصية على الانترنت؟:**

جدول (4) معرفة المستخدمين بسياسة الخصوصية على الانترنت

الإجابة	التكرار	النسبة المئوية
نعم	14	%18
لا	105	%83

يبين الجدول رقم (5) نسبة معرفة المستخدمين لمعنى سياسة الخصوصية، ومن خلال النتائج تبين أن الغالبية العظمى من عينة الدراسة لديهم دراية بموضوع سياسة الخصوصية، حيث بلغت النسبة 83% وهي نسبة عالية مقارنة بنسبة 18% الباقية. وبالرغم من أن هذه النسبة هي مؤشر جيد ولكن هذا لا يعني أنهم على دراية كافية بموضع انتهاك الخصوصية وأساليب صائدي البيانات في الحصول على بياناتهم.

هل تقرأ سياسة الخصوصية عند الاشتراك بأية خدمة في المواقع الخدمية قبل الموافقة عليها؟

توفر العديد من المواقع، خصوصاً التجارية صفحات مكتوبة لسياسة الخصوصية التي تتبعها هذه المواقع في التعامل مع بيانات المستخدمين، وبالرغم من وجود تلك الصفحات، إلا أن عدداً كبيراً من المستخدمين لا يقومون بقراءة سياسة الخصوصية لتلك المواقع ومن تم يجهلون ما هو مكتوب فيها.

جدول (5) قراءة سياسة الخصوصية قبل الموافقة عليها

الإجابة	التكرار	النسبة المئوية
نعم	54	%45
لا	65	%55

يبين الجدول رقم (6) أن أكثر من نصف أفراد العينة لا يقومون بقراءة سياسة الخصوصية الموجودة في مواقع التجارة الإلكترونية والمواقع الخدمية والتي من الممكن أن تتضمن الموافقة على تبادل بيانات المستخدمين مع المواقع الأخرى، هذه النسبة بلغت 55% من أفراد العينة.

هل تعرف ما هي العناصر الأساسية التي يجب أن تتضمنها سياسة الخصوصية بشكل عام؟

هناك العديد من الفقرات يمكن أن تضمن في سياسة الخصوصية، وهي الموافقة على تداول بيانات المستخدم أو الموافقة على إرسال رسائل دعائية عبر البريد الإلكتروني أو غير ذلك. وهناك العديد من رواد الإنترنت يقوم بقراءة سياسة الخصوصية بعجالة مما يؤدي إلى إغفال نقاط أساسية أو عدم فهمها، ومن ثمَ يؤدي إلى بعض المشاكل المتعلقة بالخصوصية.
الجدول رقم (7) يظهر أن نسبة عالية من أفراد العينة وهي 55% لا يعرفون العناصر الأساسية التي تتضمنها سياسة الخصوصية، إما أنهم يمرون على سياسة الخصوصية مرور الكرام كما ذكرنا سابقا، أو أنهم ليس لديهم دراية بموضوع سياسة الخصوصية، وهذ ما يتسبب في العديد من المشاكل التي يواجهها الزوار في بعض الأحيان.

جدول (6) الدراية بالعناصر الأساسية لسياسة الخصوصية

الإجابة	التكرار	النسبة المئوية
نعم	53	%45
لا	66	%55

هل سبق لك البحث أو التساؤل عن وجود قانون خاص بحماية الخصوصية في ليبيا؟

إن مشاكل حماية الخصوصية أوجد العديد من القوانين التي تحمي رواد الإنترنت من انتهاك الخصوصية. هناك عدد كبير من المستخدمين لديهم دراية بأن هناك قوانين في دولهم تضمن لهم الحماية من انتهاك الخصوصية ولو بشكل جزئي.

جدول (7) البحث أو التساؤل عن وجود قانون خاص بحماية الخصوصية في ليبيا

الإجابة	التكرار	النسبة المئوية
نعم	32	%27
لا	87	%73

في الجدول رقم (8) أعلاه، هناك نسبة عالية جداً بلغت 87% من أفراد العينة ليس لديهم أي دراية أو اهتمام بوجود قانون من عدمه في ليبيا، وهذا مرده إلى قلة الوعي بالأخطار المتعلقة بموضوع خصوصية البيانات.

هل ترى مشكلة في كشف أو مشاركة معلوماتك الخاصة دون إذن منك؟

جدول (8) مشكلة كشف المعلومات الخاصة دون إذن

الإجابة	التكرار	النسبة المئوية
نعم	12	%10
لا	107	%90

نسبة 90% في الجدول رقم (9) وهي نسبة عالية جدا من أفراد العينة لديهم قلق أو عدم موافقة على مشاركة البيانات الخاصة دون إذن المستخدم.

ثالثا: معرفة المستخدم بموضوع جمع بياناته وتخزينها وتداولها بين المو اقع:

هل سبق أن قام أحدهم باختراق حسابك على أحد مو اقع التواصل الاجتماعي؟

عملية جمع البيانات تتم بعدة طرق منها عملية سرقة البيانات سواء عن طريق الاختراق أو التحايل أو التتبع عبر المواقع، وقد بين الجدول رقم (10) أن نسبة 18% من أفراد العينة تعرضوا لعملية اختراق أو تحايل للولوج إلى حساباتهم في مواقع التواصل الاجتماعي، وبالرغم من أن النسبة صغيرة نوعاً ما، ولكن لأن عدد أفراد العينة يعتبر صغير بالنسبة لعدد مستخدمي الإنترنت في ليبيا، فإن نسبة 18% تعتبر نسبة مقلقة.

جدول (9) باختراق حسابك على أحد مو اقع التواصل الاجتماعي

الإجابة	التكرار	النسبة المئوية
نعم	22	%18
لا	97	%82

- هل تعرف أن مزودي الانترنت ومو اقع الإنترنت يقومون بمشاركة بياناتك الشخصية مع أطراف ثالثة (شركات بحثية/شركات دعاية وتسويق/مؤسسة أو جهة أمنية)؟

ذكرنا سابقاً أن العديد من الدراسات أظهرت أن عدداً كبيراً من بيانات المستخدمين على الانترنت يتم تداولها أو بيعها، ولذلك فإن هناك تساؤل عن معرفة رواد الإنترنت بهذا الأمر المهم.

جدول (10) مشاركة البيانات مع طرف ثالث

الإجابة	التكرار	النسبة المئوية
نعم	49	%41
لا	70	%59

أظهرت النتائج في الجدول رقم (11) أن نسبة 59% من أفراد العينة ليس لديهم معرفة بموضوع تبادل ومشاركة البيانات في مواقع الإنترنت التي يقومون بزيارتها مع أطراف أخرى قد تكون شركات بحثية أو شركات دعاية وتسويق إلكتروني أو ربما مؤسسات أمنية دون علمه. وهذا يؤدي إلى وقوع المستخدم في بعض المشاكل، أقلها الإزعاج الذي يتعرض له المستخدم بسبب الدعايات التي تحيط به في كل المواقع التي يزورها.

- هل سبق أن ظهرت لك إشعارات تفيد بأن الموقع الذي تتصفحه سيستخدم ملفات تعريف الارتباط؟

أشرنا سابقاً أن قانون ملفات تعريف الارتباط Cookies Law شدد على موضوع استخدام ملفات تعريف الارتباط وضرورة تنبيه المستخدم بأن الموقع سيستعمل هذه الملفات وانتظار موافقته عليها. وفي سؤالنا هذا أردنا معرفة نسبة الذين ظهرت لهم هذه التنبيهات من المواقع التي زاروها. الجدول رقم (12) أظهر أن ما نسبته71% من أفراد العينة أفادوا بأن هذه التنبيهات ظهرت لهم في العديد من المواقع التي زاروها، وهذا يدل على أن العديد من المواقع التزمت بتنفيذ هذا القانون.

جدول (11) إشعارات المو اقع باستخدام ملفات تعريف الارتباط

الإجابة	التكرار	النسبة المئوية
نعم	85	%71
لا	34	%29

- عندما يظهر شريط المو افقة على استخدام ملفات تعريف الارتباط أسفل الشاشة أتضغط على زر مو افق مباشرة؟ أم تقوم بتحديد ما يمكن للموقع الوصول إليه؟

إن العديد من مواقع الإنترنت التزمت بتنبيه المستخدم عند استخدامها لملفات تعريف الارتباط وطلب موافقته، حيث تظهر هذه التنبيهات إما مع طلب الموافقة المباشرة أو بالدخول لخيارات الخصوصية واختيار ما يرغب المستخدم في السماح به من بيانات للموقع.

يشير الجدول رقم (13) بأن عدداً كبيراً من أفراد العينة الذين ظهر لهم هذا التنبيه يقومون بتحديد ما يمكن الوصول إليه من بيانات تخصهم، حيث بلغت النسبة 66%. وبالرغم من أن النسبة كبيرة فإن النسبة المتبقية وهي 34% ليست صغيرة وهي التي تقوم بالموافقة مباشرة بدون مراجعة أو تخصيص الوصول لبياناتهم ومن ثم، تعرضهم لانتهاك الخصوصية بموافقتهم. وقد بين X. Hu and S. Sastry [20] أن العديد من المستخدمين وبالرغم من ظهور لائحة GDPR وقانون ملفات تعريف الارتباط فإنهم مازالوا يختارون الموافقة المباشرة على الإعدادات الافتراضية للخصوصية . وهذا يؤدي إلى وضع المزيد من ملفات تعريف الارتباط في أجهزتهم.

جدول (12) المو افقة على استخدام ملفات تعريف الارتباط

الإجابة	التكرار	النسبة المئوية
نعم	40	%34
لا	79	%66

- في حال تعرضك لسرقة أوكشف أو استغلال لمعلوماتك دون إذنك المسبق، فهل تعرف ما هي الإجراءات التي يمكنك القيام بها للمطالبة بحقك؟

العديد من الدول سنت قوانين لحماية خصوصية البيانات على الإنترنت، ولكن هذه القوانين تباينت في فاعليتها، فالعديد منها كان مجرد حبر على ورق، والبعض الآخر يشوبه الضعف في نصوصه القانونية.

من خلال النتائج التي ظهرت في الجدول رقم (14) تبين أن ما نسبته 89% لا يعرفون طريقة التصرف أو المطالبة بالحق في حال التعرض للسرقة أو الاستغلال لبياناتهم من قبل مواقع الإنترنت أو مزودي خدمة الإنترنت، وهذا مرده إلى عدم وجود قوانين بخصوص هذا الموضوع أو عدم فاعلية تلك القوانين، بالإضافة إلى غياب برامج التوعية بتلك الأخطار وكيفية الحماية منها والمطالبة بالحقوق المعنوية والمادية.

جدول (13) المطالبة بالحق في حال التعرض لسرقة أو استغلال البيانات

الإجابة	التكرار	النسبة المئوية
نعم	13	%11
لا	106	%89

- هل ترى بأن هناك حاجة لسن قانون خاص بحماية البيانات الشخصية للمواطنين في ليبيا؟

العديد من الدراسات تشير إلى أن قوانين حماية الخصوصية والملكية الفكرية في ليبيا هي قوانين ضعيفة، وأشارت إلى أن موضوع الملكية الفكرية تناول تلك القوانين في فقرات بسيطة، ولم يخصص لها قانون لوحدها بالتفصيل. حيث ذكر ج. أبوزيد [21] أن المادة 1276في القانون رقم 23 لسنة 2010 بخصوص النشاط التجاري، حددت الأعمال التي تعتبر منافسة غير مشروعة في مجالا لملكية الفكرية، ففي الفقرة الثالثة تم ذكر استغلال إنجازات الغير والحصول على المعلومات غير المفصح عنها بطرق غير مشروعة كالتجسس والسرقة والاحتيال، أما عن العقوبات فكانت عقوبات ضعيفة. يذكر م. الزوي [22] أن الدول العربية – عدا ليبيا- اهتمت بسن قوانين مخصص لحماية البيانات الشخصية والمعاملات على الفضاء الإلكتروني، وبالرغم من أن الهيئة الوطنية للأمن وسلامة المعلومات قد أصدرت بنوداً سميت بـ (السياسات الوطنية لأمن وسلامة المعلومات)، ولكنها تخص الموظفين وجهات العمل، وتبقى مجرد سياسات وليست قانوناً ملزماً لغير الموظفين[23]. حتى بوجود قانون رقم (5) لسنة 2022 والخاص بمكافحة الجريمة الإلكترونية إلا أنه لا توجد به أي مادة تشير صراحة إلى موضوع انتهاك خصوصية المستخدم من قبل الطرف الثالث[24].

الجدول رقم (15) يظهر أن الأغلبية الساحقة تؤيد فكرة وجود قوانين قوية ورادعة خاصة بحماية الخصوصية على الإنترنت في ليبيا.

جدول (14) الحاجة لسن قانون خاص بحماية البيانات الشخصية

الإجابة	التكرار	النسبة المئوية
نعم	117	%98
لا	2	%2

المناقشة

إن العالم الرقمي الكبير والذي توج بانتشار الإنترنت وهيمنته على حياتنا بشكل ملحوظ، وبالرغم من الفوائد العظيمة التي وفرها هذا العالم، إلا أن هناك جانباً خفياً في هذا العالم ، لا يعيه عدد كبير من الناس ، وهو تداول بيانات المستخدمين دون إذن منهم وانتهاك خصوصيتهم وتبادلها مع أطراف أخرى تهتم بهذه البيانات ، سواءً أكانت شركات تجارية أم دعائية وكذلك الأمنية منها ، وبالرغم من أن الدول اهتمت بهذا الجانب وسنت قوانين ولوائح لمكافحة هذه الانتهاكات ، إلا أن ليبيا ماتزال متأخرة في هذا السياق –بالرغم مع وجود بعض القوانين -. أما الجانب الآخر وهو الأهم، هو جانب وعي المستخدم نفسه بهذه الأخطار، فمن خلال الدراسة، تبين أن عدداً كبيراً من المستخدمين ليسوا على دراية بمخاطر انتهاك الخصوصية ولا يعون مدى الخطورة المترتبة على بياناتهم الشخصية.

الخلاصة

ألقت الدراسة الضوء على جانب مهم في عالم الإنترنت، ألا وهو جانب خصوصية بيانات المستخدمين الذين يرتادون الإنترنت بمئات الملايين يومياً، وما يقابله من عمليات تتبع لتلك البيانات واستغلالها بشكل قانوني وغير قانوني. تم تقسيم منهجية الدراسة إلى جزأين مهمين، جزء خاص بمراقبة مواقع الانترنت والكشف عن الأدوات التي تستخدمها للحصول على بيانات المستخدم، وجزء خاص بتحديد مدى وعي المستخدم لعملية تداول بياناته على الإنترنت وما تأتي به من مخاطر.

خلصت الدراسة إلى أن عدداً هائلاً من مواقع الإنترنت خصوصا التجارية ومواقع التواصل الاجتماعي تقوم بجمع بيانات المستخدمين، بل ومراقبة تحركاتهم خلال المواقع واستغلال تلك البيانات بطرق قانونية أو غير قانونية لتحقيق مآربها. وإلى جانب ذلك فإن العديد من المستخدمين لا يعون خطورة تلك العمليات أو ليس لديهم علم بحماية أنفسهم من تلك المخاطر بسبب غياب القوانين التي تؤمن لهم الحماية في حال حصول ذلك.

المراجع

[1] م. م. مهني، "استخدام التسويق الإلكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي،" *مجلة مستقبل العلوم الاجتماعية*، المجلد 8، 264-207. pp، 2022.

[2] أ. م. البقلي، "حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة متطلبات التجارة الإلكترونية،" *المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)*، المجلد 9، رقم 4، 1144-1002 .pp، 2021.

[3] A. K. Jain, S. R. Sahoo and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex and Intelligent Systems*, vol. 7, p. 2157–2177, 2021.

[4] J. Issak and M. J. Hanna, "User Data Privacy: FaceBook, Cambridge, Analytica and Privacy Protection," *The Policy Corner*, pp. 56-59, 2018.

[5] م. ق. مسعد، "الحماية المدنية للمعلومات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل،" *مجلة البحوث القانونية والإقتصادية*، المجلد 8، رقم 3، pp. 797-945، 2018.

[6] A. Oulasvirta, T. Suomalainen, J. Hamari, A. Lampinen and K. Karvonen, "Transparency of Intentions Decreases Privacy Concerns in Ubiquitous Surveillance," in *Cyberpsychology, Behavior, and Social Networking*, 2014.

[7] ن. سعيداني، *الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية - رسالة دكتوراه*، جامعة باتنة - كلية الحقوق، 2020.

[8] أ. جابر، "استهداف مستخدمي الإنترنت بالإعلانات التجارية وحماية الحق فى الخصوصية،" *مجلة العلوم الإنسانية*، pp. 9-46، 2015.

[9] ع. ع. الطيب، "إتجاهات الشباب السوداني نحو استغلال وسائل التواصل الإجتماعي في إنتهاك خصوصية الأفراد،" *المجلة الدولية للإتصال الإجتماعي*، المجلد 5، رقم 3، pp. 188-212، 2018.

[10] الإسكوا، "بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا،" اللجنة الاقتصادية والاجتماعية لغربي آسيا - 10 مارس 2009 - E/ESCWA/ICTD/2009/4، 2009.

[11] European Union, "General Data Protection Regulation," *Official Journal of the European Union*, 2016.

[12] "The Cookie Law Explained," 2022. [Online]. Available: www.cookieslaw.com.

[13] M. Rudolph, D. Feth and S. Polst, "Why Users Ignore Privacy Policies - A Survey and Intention Model for Explaining User Privacy Behavior," in *International Conference on Human-Computer Interaction*, 2018.

[14] S. Mittal, "User privacy and the evolution of third-party tracking mechanisms on the world wide web," 2010. [Online]. Available: https://ssrn.com/abstract=200525.

[15] A. Narayanan and D. Reisman, "The Princeton Web Transparency and Accountability Project," *Transparent data mining for Big and Small Data*, pp. 1-24, 2017.

[16] م. ت. الموسوي و ج. س. فضل الله، "الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها،" جامعة بغداد، 2013.

[17] X. Hu and N. Sastry, "What a Tangled Web We Weave: Understanding the Interconnectedness of the Third Party Cookie Ecosystem," in *WebSci*, Southampton, 2020.

[18] J. Erap, A. Anton, L. Aiman-Smith and W. Stufflebeam, "Examining Internet Privacy Policies Within the Context of User Privacy Values," *IEEE Transactions on Engineering Management*, vol. 52, no. 2, pp. 227-237, 2005.

[19] ن. جبر، م. فطافطة و د. سمارو، "خصوصيات مستباحة: تعامل الشركات المزودة للإنترنت في فلسطين مع المعلومات الشخصية للمستخدمين،" آكس ناو وإمباكت الدولية لسياسات حقوق الإنسان، 2021.

[20] X. Hu and N. Sastry, "CHARACTERISING THIRD PARTY COOKIE USAGE IN THE EU AFTER GDPR," in *11TH INTERNATIONAL ACM WEB SCIENCE CONFERENCE*, 2019.

[21] ج. ع. أبوزيد، "ثورة المعلومات في ليبيا بين عوائق تشريعية وإدارية،" تأليف *مؤتمر الأمن المعلوماتي*، طرابلس - ليبيا، 2013.

[22] الهيئة الوطنية لأمن وسلامة المعلومات، "صفحة الهيئة الوطنية لأمن ولسلامة البيانات،" Available: https://nissa.gov.ly/wp-content/uploads/NISSA_Policy_Manual_v1.0-1.pdf. [تاريخ الوصول 6 2022].

[23] المجمع القانوني الليبي، "قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية،" 27 9 2022. https://lawsociety.ly/legislation/. [تاريخ الوصول 15 10 2022].

[24] م. ع. الزوي، "الحماية الجنائية للبيانات الشخصية الإلكترونية في القانون الليبي و المقارن،" مجلة العلوم الشرعية والقانونية، رقم 1، pp. 146-231، 2018.