# تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية

م.م. صفاء خلف كريم م.م. علي رياض تمر
جامعة سومر/ رئاسة الجامعة

# The Impact of social media on Personal Privacy

Asst. Prof. Safaa Khalaf Karim Asst. Prof. Ali Riyad Tamr
Sumer University/University Presidency

**Abstract**

This academic study explores the impact of social media on personal privacy, particularly in light of its widespread global use and integration into users' daily lives. It examines the technical, psychological, social, and legal dimensions of privacy, drawing upon recent reports and specialized research. The study reviews methods of data collection and digital tracking, highlighting the risks of data leaks and privacy breaches by both platforms and third parties.It also addresses modern concepts such as "privacy fatigue," which arises from the complexity of privacy settings, and the "privacy paradox," which reflects the gap between users' behaviors and their stated concerns. Furthermore, it reveals how social media addiction can lead to negligence in safeguarding personal privacy.From a legal standpoint, the study analyzes the influence of international regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), in managing personal data usage. It also discusses the role of platform monopolies in limiting users' control over their data.The study concludes by offering practical recommendations: users should adopt safer practices, legislators must develop more effective privacy laws, and platforms need to improve transparency and data protection. Finally, the study emphasizes the importance of future research to address emerging challenges in the digital environment.

**Keywords:** social media, digital privacy, data protection, privacy fatigue, privacy paradox, digital legislation, GDPR, CCPA, user tracking, digital addiction.

**الملخص**

تناقش هذه الدراسة الأكاديمية تأثير وسائل التواصل الاجتماعي على الخصوصية الشخصية، في ظل توسع استخدامها عالميًا وتغلغلها في حياة المستخدمين اليومية. تركز الدراسة على الأبعاد التقنية والنفسية والاجتماعية والقانونية المتعلقة بخصوصية الأفراد، مستندة إلى تقارير حديثة وأبحاث علمية متخصصة. تستعرض الدراسة أساليب جمع البيانات وتقنيات التتبع الرقمية، وتسلّط الضوء على مخاطر تسريب البيانات وانتهاك الخصوصية، سواء من قبل المنصات نفسها أو من أطراف خارجية، كما تتناول الدراسة مفاهيم معاصرة مثل "إرهاق الخصوصية" الناتج عن تعقيد إعدادات الخصوصية، و"مفارقة الخصوصية" التي تشير إلى التناقض بين سلوك المستخدم

ومخاوفه المعلنة. وتُبرز الدراسة كيف يمكن لإدمان المنصات الاجتماعية أن يؤدي إلى تهاون في حماية الخصوصية الشخصية، من الجانب القانوني، تستعرض الدراسة دور التشريعات الدولية، مثل اللائحة العامة لحماية البيانات (GDPR) وقانون خصوصية المستهلك في كاليفورنيا (CCPA)، في تنظيم استخدام البيانات الشخصية. كما تدرس تأثير احتكار المنصات الرقمية على فرص حماية خصوصية المستخدمين، وفي ختامها، تقدم الدراسة مجموعة من التوصيات للمستخدمين لتبني ممارسات أكثر أمانًا، وللمشرّعين لوضع قوانين أشد فعالية، وللمنصات لتعزيز شفافيتها وحماية خصوصية مستخدميها. وتشير الدراسة إلى أهمية البحث المستقبلي لفهم أعمق للتحديات الناشئة في البيئة الرقمية.

**الكلمات المفتاحية:** وسائل التواصل الاجتماعي، الخصوصية الرقمية، حماية البيانات، إرهاق الخصوصية، مفارقة الخصوصية، التشريعات الرقمية، GDPR، CCPA، تتبع المستخدم، الإدمان الرقمي.

**المقدمة**

لقد تطور مشهد وسائل التواصل الاجتماعي بشكل كبير على مدار العقدين الماضيين، من كونه منصة بسيطة للتواصل مع الأصدقاء إلى أداة قوية للتواصل ومشاركة المحتوى والعمليات التجارية ونشر الأخبار والمعلومات، ووفقًا لتقرير Digital 2022: A Global Overview، سيصل عدد مستخدمي وسائل التواصل الاجتماعي النشطين إلى ما يقرب من ٤،٦ مليار في عام ٢٠٢٢، وهو ما يمثل أكثر من ٥٨٪ من إجمالي سكان العالم (Neves et al.، 2024)، تشمل المنصات الأكثر شهرة Facebook وInstagram وTikTok وSnapchat وYouTube وTwitter وLinkedIn، بالإضافة إلى تطبيقات المواعدة مثل Grindr وTinder.

ومع ذلك، فإن التطور السريع لوسائل التواصل الاجتماعي قد منحها تأثيرًا ووصولًا استثنائيين في حياة المستخدمين، تجمع شركات وسائل التواصل الاجتماعي بيانات حساسة حول الأنشطة الشخصية والاهتمامات وسمات الشخصية والآراء السياسية وعادات الشراء والسلوك عبر الإنترنت، في كثير من الحالات، تُستخدم هذه البيانات لزيادة تفاعل المستخدم من خلال الخوارزميات وبيع الإعلانات السلوكية – والتي غالبًا ما يكون لها آثار مشوهة وتمييزية (EPIC، بدون تاريخ).

مع تزايد حجم البيانات الشخصية التي تُجمع وتُعالج وتُخزن، تتزايد أهمية الخصوصية الشخصية في العصر الرقمي، أصبحت الخصوصية حقًا أساسيًا من حقوق الإنسان في العديد من القوانين الدولية، إذ تُمثل قدرة الأفراد على التحكم في معلوماتهم الشخصية وتحديد من يمكنه الوصول إليها واستخدامها، ومع ذلك، تُشكل طبيعة وسائل التواصل الاجتماعي المفتوحة والمُشاركة تحديات فريدة للخصوصية الشخصية.

**المبحث الأول: الإطار المنهجي للبحث**

**١.٢ إشكالية البحث**

السؤال البحثي هو التناقض بين الرغبة في التفاعل الاجتماعي على منصات التواصل الاجتماعي والحاجة إلى الحفاظ على الخصوصية الشخصية، يواجه مستخدمو وسائل التواصل الاجتماعي مفارقة تتعلق بالخصوصية، حيث يعبرون عن مخاوفهم بشأن الخصوصية من جهة، لكنهم يواصلون الكشف عن معلوماتهم الشخصية على هذه المنصات من جهة أخرى، في السنوات الأخيرة، وقعت العديد من حوادث انتهاكات الخصوصية عبر الإنترنت الناجمة عن تسريب المعلومات الشخصية لمستخدمي وسائل التواصل الاجتماعي، على سبيل المثال، أفادت وسائل الإعلام البريطانية أن البيانات الشخصية لـ ٨٧ مليون مستخدم على فيسبوك قد سُرّبت بشكل غير قانوني إلى شركة الاستشارات السياسية كامبريدج أناليتيكا (ريفيل، ٢٠١٩)، بالإضافة إلى ذلك، أبلغت شركة إيكويفاكس، إحدى وكالات الائتمان الرئيسية الثلاث في الولايات المتحدة، عن خرق واسع النطاق للبيانات في عام ٢٠١٧ شمل ١٤٦ مليون معلومة شخصية (تشو وشوب، ٢٠١٨).

لقد رفعت هذه الأحداث الوعي بمخاطر الخصوصية، لكنها أدت أيضًا إلى ظهور ما يُعرف بـ"إرهاق الخصوصية"، حيث يشعر المستخدمون بالإرهاق والإحباط عند محاولتهم حماية خصوصيتهم، مما يؤدي إلى المزيد من انتهاكات الخصوصية والدخول في حلقة مفرغة (تشن وآخرون، ٢٠٢٣)، وقد تفاقمت هذه المشكلة بسبب عدة عوامل: ١. سياسات الخصوصية معقدة ويصعب فهمها؛ ٢. تتغير سياسات الخصوصية باستمرار دون إعلام المستخدمين بوضوح؛ ٣. انعدام الشفافية في كيفية جمع البيانات واستخدامها؛ ٤. تركيز السوق واحتكار منصات التواصل الاجتماعي يحدّان من خيارات المستخدمين؛ ٥. إدمان وسائل التواصل الاجتماعي يعيق قدرة المستخدمين على اتخاذ قرارات عقلانية بشأن خصوصيتهم.

**١.٣ أهداف البحث**

يهدف هذا البحث إلى تحقيق الأهداف التالية:

١. تحليل آليات جمع البيانات في مواقع التواصل الاجتماعي: دراسة الطرق المختلفة التي تستخدمها منصات التواصل الاجتماعي لجمع البيانات الشخصية للمستخدمين، سواء كانت بيانات مقدمة طوعاً، أو بيانات سلوكية، أو بيانات مستنتجة.

٢. دراسة التأثيرات النفسية والاجتماعية لانتهاكات الخصوصية: استكشاف ظواهر مثل إرهاق الخصوصية، وتأثير إدمان مواقع التواصل الاجتماعي على قرارات حماية الخصوصية، والسلوكيات التصحيحية التي يتبناها المستخدمون للتعامل مع مخاوف الخصوصية.

٣. استكشاف الإطار القانوني والتنظيمي لحماية الخصوصية: تحليل التشريعات العالمية لحماية الخصوصية، وتأثير احتكار منصات التواصل الاجتماعي على الخصوصية، والحاجة إلى تشريعات شاملة لحماية البيانات.
٤. تقديم استراتيجيات فعالة لحماية الخصوصية الشخصية: اقتراح تدخلات وإستراتيجيات عملية لمساعدة المستخدمين على حماية خصوصيتهم، مثل تدخلات إثارة الخوف من انتهاك الخصوصية، ودور التركيز التنظيمي في حماية الخصوصية.

**١.٤ منهجية البحث**

يعتمد هذا البحث على المنهج الوصفي التحليلي، الذي يقوم على جمع البيانات والمعلومات من المصادر المختلفة، وتحليلها وتفسيرها للوصول إلى استنتاجات علمية. تم الاعتماد على مجموعة متنوعة من المصادر، تشمل:

١. الدراسات الأكاديمية المحكمة: تم الاستناد إلى دراسات حديثة منشورة في مجلات علمية محكمة، مثل دراسة Chen et al، (٢٠٢٣) حول آلية تأثير تجارب انتهاك الخصوصية على نوايا حماية الخصوصية، ودراسة Neves et al، (٢٠٢٤) حول مخاوف الخصوصية في استخدام وسائل التواصل الاجتماعي.
٢. التقارير المتخصصة: تم الاستفادة من تقارير المنظمات المتخصصة في مجال الخصوصية الرقمية، مثل تقارير المركز الإلكتروني لمعلومات الخصوصية (EPIC).
٣. الإحصائيات والبيانات الحديثة: تم الاستناد إلى إحصائيات حديثة حول استخدام مواقع التواصل الاجتماعي وانتهاكات الخصوصية، مثل تقرير "Digital 2022: Global Overview Report".
٤. دراسات الحالة: تم تحليل بعض حالات انتهاك الخصوصية البارزة، مثل قضية كامبريدج أناليتيكا وفيسبوك، وتسريب بيانات إكويفاكس.

تتمثل حدود البحث في التركيز على تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية، دون التطرق بشكل مفصل إلى قضايا الأمن السيبراني أو الجرائم الإلكترونية، كما يركز البحث على الدراسات والتقارير المنشورة في الفترة من ٢٠١٨ إلى ٢٠٢٤، لضمان حداثة المعلومات والبيانات، تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية.

**المبحث الثاني: الإطار النظري للدراسة**

**أولاً: مفهوم الخصوصية في سياق مواقع التواصل الاجتماعي**

تعد الخصوصية مفهوماً متعدد الأبعاد يتطور باستمرار مع تطور التكنولوجيا والمجتمع، في سياق مواقع التواصل الاجتماعي، تكتسب الخصوصية أبعاداً جديدة تختلف عن المفهوم التقليدي للخصوصية في العالم المادي.

يمكن تعريف الخصوصية الرقمية بأنها قدرة الفرد على التحكم في المعلومات الشخصية التي يشاركها عبر الإنترنت، وتحديد من يمكنه الوصول إليها واستخدامها، وفي أي سياق (Baldwin et al., 2023).

تتميز الخصوصية في بيئة مواقع التواصل الاجتماعي بعدة خصائص فريدة منها:

١. الطبيعة الدائمة للمعلومات: على عكس التفاعلات في العالم المادي، فإن المعلومات المشاركة عبر مواقع التواصل الاجتماعي غالباً ما تكون دائمة ويمكن الوصول إليها لفترات طويلة.
٢. قابلية البحث والاسترجاع: يمكن البحث عن المعلومات الشخصية واسترجاعها بسهولة باستخدام محركات البحث وأدوات التحليل.
٣. قابلية النسخ والمشاركة: يمكن نسخ المحتوى الرقمي ومشاركته بسهولة، مما يجعل من الصعب التحكم في انتشاره بمجرد مشاركته.
٤. الجمهور غير المرئي: غالباً ما يكون من الصعب تحديد من يمكنه الوصول إلى المعلومات الشخصية في بيئة مواقع التواصل الاجتماعي.
٥. تداخل السياقات: تجمع مواقع التواصل الاجتماعي بين سياقات مختلفة (مهنية، شخصية، عائلية) في منصة واحدة، مما يخلق تحديات في إدارة الخصوصية.

يختلف مفهوم الخصوصية الرقمية عن الخصوصية التقليدية في عدة جوانب، في العالم المادي، غالباً ما ترتبط الخصوصية بالمساحة المادية والحدود الفيزيائية، مثل منزل الشخص أو مكتبه، أما في العالم الرقمي، فإن الخصوصية تتجاوز الحدود المادية لتشمل المساحات الافتراضية والبيانات الرقمية، كما أن الخصوصية التقليدية غالباً ما تكون ثنائية (إما خاصة أو عامة)، بينما الخصوصية الرقمية أكثر تعقيداً وتدرجاً، حيث يمكن مشاركة المعلومات مع مجموعات مختلفة بمستويات مختلفة من الوصول.

ومن المصطلحات المرتبطة بمفهوم الخصوصية يأتي مفهوم مخاوف الخصوصية والتي تعرف بأنها "مدى قلق المستخدم بشأن ممارسات المواقع المتعلقة بجمع واستخدام معلوماته الشخصية" (Hong & Thong, 2013).

وقد حددت الدراسات عدة أنواع رئيسية لمخاوف الخصوصية في سياق مواقع التواصل الاجتماعي:

١. مخاوف جمع البيانات: تتعلق بالقلق بشأن كمية البيانات الشخصية التي تجمعها مواقع التواصل الاجتماعي وطريقة جمعها، وفقاً لـ(Neves et al. ٢٠٢٤)، يشعر المستخدمون بالقلق من أن منصات التواصل الاجتماعي تجمع بيانات أكثر مما هو ضروري لتقديم خدماتها، وغالباً دون علم المستخدم أو موافقته الصريحة.
٢. مخاوف الاستخدام الثانوي للبيانات: تتعلق بالقلق بشأن استخدام البيانات الشخصية لأغراض أخرى غير تلك التي تم جمعها من أجلها، على سبيل المثال، قد تستخدم منصات التواصل الاجتماعي بيانات

المستخدمين لأغراض الإعلانات المستهدفة أو بيعها لأطراف ثالثة، كما أشار تقرير EPIC، "في كثير من الحالات تُستخدم هذه البيانات لدفع مشاركة المستخدمين بشكل خوارزمي وبيع الإعلانات السلوكية – غالباً مع تأثيرات مشوهة وتمييزية" (EPIC, n.d.).

٣. مخاوف الوصول غير المصرح به: تتعلق بالقلق بشأن وصول أشخاص أو جهات غير مصرح لها إلى البيانات الشخصية، سواء من خلال الاختراق أو الثغرات الأمنية أو سوء إدارة الصلاحيات، وفقاً لدراسة (Chen et al. ٢٠٢٣)، فإن حوادث تسريب البيانات المتكررة، مثل حادثة كامبريدج أناليتيكا، قد زادت من هذه المخاوف لدى المستخدمين.

٤. مخاوف الأخطاء في البيانات: تتعلق بالقلق بشأن دقة البيانات الشخصية المخزنة وإمكانية تصحيحها، قد تؤدي الأخطاء في البيانات إلى عواقب سلبية، مثل الاستهداف الخاطئ أو التمييز غير المبرر.

٥. مخاوف فقدان السيطرة: تتعلق بالقلق بشأن عدم القدرة على التحكم في من يمكنه الوصول إلى البيانات الشخصية وكيفية استخدامها، كما أشار (Chen et al. ٢٠٢٣)، "مع زيادة تكرار خروقات البيانات على الإنترنت، يجد الناس أنهم يتمتعون بسيطرة أقل على بياناتهم".

٦. مخاوف الوعي بممارسات الخصوصية: تتعلق بالقلق بشأن عدم وضوح سياسات الخصوصية وصعوبة فهمها، وفقاً لـ(Baldwin et al. ٢٠٢٣)، "العديد من منصات التواصل الاجتماعي تحدد نواياها حول معلومات المستخدمين واهتمامات الخصوصية في اتفاقيات شروط الخدمة؛ ومع ذلك، نظراً لأن العديد من هذه الاتفاقيات طويلة وصعبة الفهم، فإن غالبية المستخدمين لا يأخذون الوقت لقراءتها".

تختلف شدة هذه المخاوف باختلاف العوامل الديموغرافية والثقافية والشخصية، على سبيل المثال، وجدت دراسة(Chen et al. ٢٠٢٣) أن الأفراد ذوي التركيز الوقائي (Prevention–focus) أكثر عرضة للشعور بإرهاق الخصوصية من أولئك ذوي التركيز الترويجي (Promotion–focus).

**ثانياً: النظريات المفسرة لسلوك الخصوصية**

هناك عدة نظريات تساعد في فهم سلوك الخصوصية لدى مستخدمي مواقع التواصل الاجتماعي يمكن إجمالها بالآتي:

**١–نظرية حماية الدافع (Protection Motivation Theory – PMT)**

تعد نظرية حماية الدافع من النظريات الشائعة في دراسات الخصوصية عبر الإنترنت ( Chen et al., 2015)، وفقاً (لروجرز ١٩٧٥)، يقوم الأفراد بتقييم المخاطر معرفياً قبل تبني سلوكيات معينة، وتطوير دافع الحماية، وفي النهاية تعديل سلوكياتهم لتجنب المخاطر.

تقترح النظرية أن هناك مصدرين للتأثير على تقييمات الأفراد للاستجابة: المصدر البيئي والمصدر الشخصي، يتضمن المصدر البيئي التهديدات الخارجية، مثل انتهاكات الخصوصية السابقة، بينما يتضمن المصدر الشخصي العوامل النفسية الداخلية، مثل الكفاءة الذاتية والتوجه التنظيمي.

في سياق الخصوصية في مواقع التواصل الاجتماعي، تفسر هذه النظرية كيف يمكن لتجارب انتهاك الخصوصية السابقة أن تؤثر على نوايا المستخدمين لحماية خصوصيتهم، وفقاً لدراسة (Chen et al. ٢٠٢٣)، "يمكن لتجارب انتهاك الخصوصية السابقة لمستخدمي وسائل التواصل الاجتماعي أن تزيد من نيتهم لحماية الخصوصية، وتتوسط هذه العملية تكاليف الاستجابة وإرهاق الخصوصية".

ومع ذلك، فقد اقترحت الدراسات الحديثة أن نظرية حماية الدافع يمكن تحسينها من خلال إدخال عوامل عاطفية فردية، مثل إرهاق الخصوصية (Mousavi et al., 2020).

**٢- نظرية التركيز التنظيمي (Regulatory Focus Theory)**

تقترح نظرية التركيز التنظيمي أن الأفراد ينظمون سلوكياتهم وفقاً لتوجهين تنظيميين مختلفين: التركيز الترويجي (Promotion-focus) والتركيز الوقائي (Prevention-focus).

الأفراد ذوو التركيز الترويجي يميلون إلى التركيز على تحقيق الأهداف والطموحات والمكاسب المحتملة، في سياق الخصوصية، قد يركز هؤلاء الأفراد على الفوائد المحتملة من مشاركة المعلومات الشخصية، مثل التواصل الاجتماعي وبناء العلاقات.

أما الأفراد ذوو التركيز الوقائي فيميلون إلى التركيز على تجنب المخاطر والخسائر المحتملة والالتزام بالواجبات والمسؤوليات، في سياق الخصوصية، قد يركز هؤلاء الأفراد على المخاطر المحتملة من مشاركة المعلومات الشخصية، مثل انتهاك الخصوصية والاحتيال.

وفقاً لدراسة (Chen et al. ٢٠٢٣)، "الأفراد ذوو التركيز الترويجي أقل عرضة للشعور بإرهاق الخصوصية من أولئك ذوي التركيز الوقائي"، وهذا يشير إلى أن التركيز التنظيمي يمكن أن يؤثر على كيفية استجابة الأفراد لمخاوف الخصوصية وتجارب انتهاك الخصوصية.

**٣- نظرية المقايضة بين الخصوصية والفائدة (Privacy-Utility Tradeoff Theory)**

تقترح هذه النظرية أن الأفراد يوازنون بين قيمة الخصوصية والفوائد المتوقعة من الكشف عن المعلومات الشخصية، في سياق مواقع التواصل الاجتماعي، قد يقرر المستخدمون الكشف عن معلومات شخصية معينة مقابل فوائد مثل الوصول إلى خدمات مجانية، أو تخصيص المحتوى، أو تعزيز التفاعل الاجتماعي.

وفقاً لـ(Neves et al. ٢٠٢٤)، "على الرغم من أن الناس يمكن أن يربطوا النتائج السلبية باستخدام مواقع التواصل الاجتماعي، إلا أنهم لا يستطيعون اجتماعياً ومهنياً التخلي تماماً عن استخدام مواقع التواصل الاجتماعي"،

هذا يشير إلى أن المستخدمين غالباً ما يضطرون إلى المقايضة بين خصوصيتهم والفوائد الاجتماعية والمهنية لاستخدام مواقع التواصل الاجتماعي.

تساعد هذه النظريات مجتمعة في فهم السلوكيات المعقدة للمستخدمين تجاه الخصوصية في مواقع التواصل الاجتماعي، وتوفر إطاراً نظرياً لتطوير استراتيجيات فعالة لحماية الخصوصية الشخصية، تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية

**ثالثاً: آليات جمع البيانات والتهديدات التقنية**

تستخدم منصات التواصل الاجتماعي مجموعة متنوعة من الآليات لجمع البيانات الشخصية للمستخدمين، يمكن تصنيف هذه البيانات إلى ثلاث فئات رئيسية:

**١ – البيانات المقدمة طوعاً**

هي المعلومات التي يقدمها المستخدمون بشكل مباشر وطوعي عند إنشاء حساباتهم أو استخدام المنصات، تشمل هذه البيانات:

المعلومات الشخصية الأساسية: الاسم، تاريخ الميلاد، الجنس، العنوان، رقم الهاتف، البريد الإلكتروني:

- المحتوى المنشور: المنشورات، الصور، مقاطع الفيديو، التعليقات، الرسائل الخاصة.
- معلومات الملف الشخصي: السيرة الذاتية، المؤهلات التعليمية، الخبرات المهنية، الاهتمامات، الحالة الاجتماعية.
- العلاقات الاجتماعية: قوائم الأصدقاء، المتابعين، المجموعات المنضم إليها.

وفقاً لتقرير EPIC، "شركات التواصل الاجتماعي تجمع بيانات حساسة عن أنشطة الأفراد واهتماماتهم وخصائصهم الشخصية وآرائهم السياسية وعادات الشراء والسلوكيات عبر الإنترنت" (EPIC, n.d.)، هذه البيانات، رغم أنها مقدمة طوعاً، غالباً ما يتم جمعها دون فهم كامل من المستخدمين لكيفية استخدامها لاحقاً.

**٢ – البيانات السلوكية**

هي المعلومات التي تجمعها المنصات عن سلوك المستخدمين وتفاعلاتهم داخل المنصة، دون تقديمها بشكل مباشر، تشمل هذه البيانات:

- أنماط الاستخدام: وقت وتكرار الدخول، مدة الجلسات، الأجهزة المستخدمة.
- التفاعلات: الإعجابات، المشاركات، التعليقات، الردود، الرسائل.
- سلوك التصفح: المحتوى الذي يتم عرضه، الوقت المستغرق في مشاهدة منشور معين، التمرير والتوقف.
- الموقع الجغرافي: بيانات GPS، المواقع المتكررة، أنماط التنقل.

كما أشار (Neves et al. ٢٠٢٤)، "تستخدم هذه البيانات لدفع مشاركة المستخدمين بشكل خوارزمي وبيع الإعلانات السلوكية – غالباً مع تأثيرات مشوهة وتمييزية"، هذه البيانات السلوكية تمكن المنصات من بناء نماذج تنبؤية دقيقة عن سلوك المستخدمين واهتماماتهم.

**٣- البيانات المستنتجة**

هي المعلومات التي تستنتجها المنصات من خلال تحليل البيانات المقدمة طوعاً والبيانات السلوكية باستخدام خوارزميات الذكاء الاصطناعي والتعلم الآلي، تشمل هذه البيانات:

- التفضيلات والاهتمامات: الميول السياسية، الاهتمامات الترفيهية، التفضيلات الاستهلاكية.
- الخصائص النفسية: السمات الشخصية، الحالة المزاجية، مستويات التوتر والقلق.
- التوجهات: الآراء المحتملة حول قضايا معينة، احتمالية الاستجابة لإعلان معين.
- العلاقات والروابط: العلاقات غير المعلنة، الشبكات الاجتماعية الخفية.

وفقاً لتقرير المفوض السابق للجنة التجارة الفيدرالية روهيت شوبرا، "يمكن لفيسبوك تطوير صورة مفصلة وحميمة لكل مستخدم يتم تحديثها باستمرار في الوقت الفعلي، بما في ذلك سلوك المشاهدة، وردود أفعالنا تجاه أنواع معينة من المحتوى، وأنشطتنا عبر المجال الرقمي حيث يتم تضمين تقنية فيسبوك" (EPIC, n.d.).

**٤- تقنيات التتبع والمراقبة**

تستخدم منصات التواصل الاجتماعي مجموعة متنوعة من التقنيات لتتبع المستخدمين ومراقبة سلوكهم، سواء داخل المنصات أو خارجها، ومنها ملفات تعريف الارتباط هي ملفات نصية صغيرة يتم تخزينها على جهاز المستخدم وتستخدم لتتبع نشاطه عبر الإنترنت، تستخدم منصات التواصل الاجتماعي عدة أنواع من ملفات تعريف الارتباط:

- ملفات تعريف الارتباط الأساسية: ضرورية لتشغيل الموقع وتوفير الخدمات الأساسية.
- ملفات تعريف الارتباط التحليلية: تجمع معلومات حول كيفية استخدام الموقع لتحسين الأداء.
- ملفات تعريف الارتباط الوظيفية: تتذكر تفضيلات المستخدم وإعداداته.
- ملفات تعريف الارتباط الإعلانية: تتبع سلوك التصفح لتقديم إعلانات مستهدفة.
- ملفات تعريف الارتباط من الطرف الثالث: توضع من قبل مواقع أخرى غير الموقع الذي يزوره المستخدم، وتستخدم للتتبع عبر مواقع متعددة.

كما أشار تقرير EPIC، "الجدير بالذكر أن التتبع والإعلانات السلوكية من قبل شركات وسائل التواصل الاجتماعي لا تقتصر على المنصات نفسها، تستخدم شركات مثل فيسبوك تقنيات تتبع يصعب اكتشافها لمتابعة الأفراد عبر مجموعة متنوعة من التطبيقات والمواقع والأجهزة" (EPIC, n.d.).

ومنها أيضاً بصمة المتصفح وهي تقنية تجمع معلومات عن متصفح المستخدم وجهازه لإنشاء معرف فريد يمكن استخدامه للتتبع، على عكس ملفات تعريف الارتباط، لا يمكن حذف بصمات المتصفح بسهولة، تشمل المعلومات المستخدمة في بصمة المتصفح كل من نوع وإصدار المتصفح- نظام التشغيل والإصدار- الإضافات المثبتة- الإعدادات اللغوية- دقة الشاشة وعمق الألوان- المكونات الإضافية المثبتة- منطقة التوقيت

**٥- تقنيات التتبع عبر الأجهزة المختلفة**

تستخدم منصات التواصل الاجتماعي تقنيات متقدمة لربط نشاط المستخدم عبر أجهزة مختلفة (الهاتف، الكمبيوتر، الجهاز اللوحي)، مما يسمح بتتبع شامل لسلوك المستخدم، تشمل هذه التقنيات:

- التتبع المستند إلى الحساب: ربط النشاط بحساب المستخدم عندما يسجل الدخول على أجهزة مختلفة.
- التتبع المستند إلى الإحصائيات: استخدام خوارزميات إحصائية لربط الأجهزة المختلفة بناءً على أنماط الاستخدام المتشابهة.
- التتبع المستند إلى الشبكة: ربط الأجهزة التي تتصل بنفس شبكة Wi-Fi أو تظهر من نفس عنوان IP.

**رابعاً: نماذج عن حالات تسرب البيانات في مواقع التواصل الاجتماعي**

تم تسجيل العديد من حالات تسرب البيانات الخاصة بمستخدمي مواقع التواصل الاجتماعي منذ بداية توظيفها إلى اليوم، ونذكر منها:

**١- تسريب بيانات فيسبوك (٢٠١٩)**

في أبريل ٢٠١٩، تم اكتشاف أن بيانات أكثر من ٥٤٠ مليون مستخدم لفيسبوك كانت معرضة على خوادم أمازون العامة، تضمنت البيانات المسربة معرفات المستخدمين، والتعليقات، والإعجابات، وردود الفعل، والأسماء الحقيقية، كان هذا التسريب نتيجة لتطبيقات طرف ثالث جمعت بيانات من فيسبوك وخزنتها على خوادم غير آمنة.

**٢- تسريب بيانات لينكد إن (٢٠٢١)**

في أبريل ٢٠٢١، تم تسريب بيانات أكثر من ٥٠٠ مليون مستخدم للينكد إن، بما في ذلك أسماء المستخدمين، وعناوين البريد الإلكتروني، وأرقام الهواتف، والمسميات الوظيفية، تم عرض هذه البيانات للبيع على منتديات القرصنة.

**خامساً: تداعيات تسريب البيانات الشخصية**

تسريب البيانات الشخصية يمكن أن يكون له عواقب وخيمة على المستخدمين:

- سرقة الهوية: يمكن استخدام البيانات المسربة لانتحال هوية الضحايا وارتكاب جرائم باسمهم.
- الاحتيال المالي: يمكن استخدام المعلومات الشخصية للوصول إلى الحسابات المصرفية أو بطاقات الائتمان.

- التصيد الاحتيالي المستهدف: يمكن استخدام البيانات المسربة لإنشاء هجمات تصيد احتيالي مخصصة ومقنعة.
- الابتزاز والتحرش: يمكن استخدام المعلومات الحساسة للابتزاز أو التحرش.
- الضرر السمعي: يمكن أن يؤدي تسريب معلومات خاصة إلى الإضرار بسمعة الشخص مهنياً واجتماعياً.

**سادساً: التأثيرات النفسية والاجتماعية**

يؤدي تسريب البيانات الشخصية لمجموعة من التداعيات النفسية والاجتماعية ومنها:

**١- إرهاق الخصوصية**

يعد "إرهاق الخصوصية" (Privacy Fatigue) من المفاهيم الحديثة نسبياً في دراسات الخصوصية الرقمية، ويشير إلى حالة من الإرهاق والإحباط والاستسلام التي يشعر بها المستخدمون نتيجة الجهود المستمرة والمرهقة لحماية خصوصيتهم في البيئة الرقمية، وفقاً لـ (Choi et al. ٢٠١٨)، يمكن تعريف إرهاق الخصوصية بأنه "حالة من الإرهاق العاطفي والسلبية والاستسلام المرتبطة بالإجراءات المستمرة المطلوبة لحماية الخصوصية الشخصية".

**أسباب إرهاق الخصوصية**

هناك عدة عوامل تساهم في تطور إرهاق الخصوصية لدى مستخدمي مواقع التواصل الاجتماعي:

١. تعقيد إعدادات الخصوصية: غالباً ما تكون إعدادات الخصوصية في مواقع التواصل الاجتماعي معقدة وصعبة الفهم، مما يتطلب جهداً كبيراً من المستخدمين لفهمها وتخصيصها.
٢. التغييرات المتكررة في سياسات الخصوصية: تقوم منصات التواصل الاجتماعي بتحديث سياسات الخصوصية بشكل متكرر، مما يتطلب من المستخدمين مراجعة وفهم هذه التغييرات باستمرار.
٣. كثرة حوادث انتهاك الخصوصية: مع تزايد حوادث تسريب البيانات وانتهاكات الخصوصية، يشعر المستخدمون بأن جهودهم لحماية خصوصيتهم غير مجدية.
٤. الشعور بقلة السيطرة: كما أشار (Chen et al. ٢٠٢٣)، "مع زيادة تكرار خروقات البيانات على الإنترنت، يجد الناس أنهم يتمتعون بسيطرة أقل على بياناتهم، علاوة على ذلك، فإنهم مرهقون من اضطرارهم لحماية خصوصيتهم بمفردهم".
٥. تكاليف الاستجابة العالية: تشير تكاليف الاستجابة إلى الجهد والوقت والموارد المطلوبة لاتخاذ إجراءات حماية الخصوصية، عندما تكون هذه التكاليف مرتفعة، يزداد احتمال شعور المستخدمين بإرهاق الخصوصية.

**٢- تغيير إعدادات الخصوصية**

يقوم العديد من المستخدمين بتعديل إعدادات الخصوصية الخاصة بهم للحد من كمية المعلومات التي يشاركونها وتحديد من يمكنه الوصول إليها، وفقاً لـ(Neves et al. ٢٠٢٤)، "مستخدمو مواقع التواصل الاجتماعي سيغيرون سلوكهم لضمان الحفاظ على خصوصية معلوماتهم".

تشمل التغييرات الشائعة في إعدادات الخصوصية:

- تقييد من يمكنه رؤية المنشورات والمعلومات الشخصية.
- تعطيل ميزات تتبع الموقع.
- تقييد استخدام البيانات الشخصية للإعلانات المستهدفة.
- مراجعة وإدارة التطبيقات والمواقع المرتبطة بحسابات التواصل الاجتماعي.
- تفعيل المصادقة الثنائية لتعزيز أمان الحساب

**سابعاً: الجوانب القانونية والتنظيمية**

تشهد سوق منصات التواصل الاجتماعي تركيزاً كبيراً، حيث تسيطر عدد قليل من الشركات الكبرى على غالبية المستخدمين والإيرادات، هذا التركيز في السوق له تأثيرات عميقة على خصوصية المستخدمين.

كما تتميز سوق منصات التواصل الاجتماعي بظاهرة "الفائز يأخذ كل شيء" (Winner-takes-all)، حيث تستفيد المنصات الكبرى من تأثيرات الشبكة: كلما زاد عدد المستخدمين، زادت قيمة المنصة للمستخدمين الجدد، هذه الديناميكية أدت إلى هيمنة عدد قليل من الشركات على السوق، مثل Meta (المالكة لفيسبوك، إنستغرام، واتساب)، وAlphabet (المالكة لجوجل ويوتيوب)، و.TikTok

كما أشار تقرير EPIC، "تتفاقم مخاطر الخصوصية للشبكات الاجتماعية من خلال تركيز المنصات، مما مكّن بعض شركات وسائل التواصل الاجتماعي من الاستحواذ على المنافسين وممارسة القوة الاحتكارية والحد بشدة من ظهور بدائل تحمي الخصوصية" (EPIC, n.d.).

استراتيجية الاستحواذ على المنافسين الناشئين هي إحدى الطرق التي تحافظ بها الشركات الكبرى على هيمنتها. على سبيل المثال:

- استحواذ فيسبوك على إنستغرام (٢٠١٢) مقابل ١ مليار دولار
- استحواذ فيسبوك على واتساب (٢٠١٤) مقابل ١٩ مليار دولار
- استحواذ مايكروسوفت على لينكد إن (٢٠١٦) مقابل ٢٦.٢ مليار دولار

هذه الاستحواذات لا تؤدي فقط إلى تركيز السوق، بل تسمح أيضاً للشركات الكبرى بدمج قواعد بيانات المستخدمين وتوسيع نطاق جمع البيانات.

**تأثير الاحتكار على خيارات المستخدمين**

يؤثر احتكار منصات التواصل الاجتماعي على خيارات المستخدمين فيما يتعلق بالخصوصية بعدة طرق:

١. محدودية البدائل: مع سيطرة عدد قليل من الشركات على السوق، يجد المستخدمون خيارات محدودة للمنصات التي تقدم ضمانات أفضل للخصوصية.
٢. القوة غير المتكافئة في المفاوضات: يضطر المستخدمون للقبول بشروط الخدمة وسياسات الخصوصية التي تفرضها المنصات الكبرى، دون القدرة على التفاوض أو التأثير عليها.
٣. تكاليف التبديل العالية: مع تركيز معظم الشبكات الاجتماعية للمستخدم في منصة واحدة أو عدد قليل من المنصات، تصبح تكاليف الانتقال إلى منصات بديلة مرتفعة (فقدان الاتصالات، المحتوى، التاريخ).
٤. عدم قابلية التشغيل البيني: غالباً ما تفتقر منصات التواصل الاجتماعي إلى القدرة على التشغيل البيني، مما يعني أن المستخدمين لا يستطيعون التواصل عبر منصات مختلفة، مما يعزز تأثير الشبكة ويزيد من تركيز السوق.

كما أشار تقرير EPIC، "يجد المستخدمون أنفسهم مضطرين للاختيار بين الانسحاب من المشاركة الاجتماعية عبر الإنترنت تماماً أو قبول شروط الخدمة التي تسمح بجمع البيانات الشخصية واستخدامها بطرق تنتهك خصوصيتهم" (EPIC, n.d.).

**دراسة حالة:** استحواذ فيسبوك على واتساب وتغيير سياسات الخصوصية

تعد قضية استحواذ فيسبوك على واتساب وما تبعها من تغييرات في سياسات الخصوصية مثالاً واضحاً على تأثير الاحتكار على خصوصية المستخدمين:

١. في عام ٢٠١٤، استحوذت فيسبوك على واتساب مقابل ١٩ مليار دولار.
٢. عند الاستحواذ، وعدت فيسبوك بالحفاظ على استقلالية واتساب وعدم دمج بيانات المستخدمين.
٣. في عام ٢٠١٦، أعلن واتساب عن تغيير في سياسة الخصوصية، مما سمح بمشاركة بيانات المستخدمين مع فيسبوك.
٤. في عام ٢٠٢١، أعلن واتساب عن تحديث آخر لسياسة الخصوصية، مما أثار مخاوف واسعة بشأن مشاركة البيانات مع فيسبوك.
٥. واجه المستخدمون خياراً صعباً: قبول السياسة الجديدة أو فقدان إمكانية استخدام التطبيق، مما يوضح القوة غير المتكافئة في المفاوضات.

هذه القضية توضح كيف يمكن للشركات المهيمنة استغلال قوتها السوقية لفرض تغييرات في سياسات الخصوصية، مع توفير خيارات محدودة للمستخدمين.

**ثامناً: التشريعات العالمية لحماية الخصوصية**

في مواجهة التحديات المتزايدة للخصوصية في العصر الرقمي، طورت العديد من الدول والمناطق تشريعات لحماية خصوصية البيانات. فيما يلي نظرة على أبرز هذه التشريعات:

اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي

تعد اللائحة العامة لحماية البيانات (GDPR)، التي دخلت حيز التنفيذ في مايو ٢٠١٨، من أشمل وأكثر التشريعات صرامة في مجال حماية البيانات، تنطبق على جميع الشركات التي تعالج بيانات مواطني الاتحاد الأوروبي، بغض النظر عن موقع الشركة.

كما أشار تقرير EPIC، "يجب على الكونغرس سن تشريعات شاملة لحماية البيانات لوضع قيود صارمة على جمع البيانات الشخصية ومعالجتها واستخدامها والاحتفاظ بها من قبل الشبكات الاجتماعية والكيانات الأخرى" (EPIC, n.d.)، فيما يلي بعض المقترحات لتطوير الإطار التنظيمي:

١. تشريعات فيدرالية شاملة: في الولايات المتحدة، هناك حاجة إلى تشريع فيدرالي شامل لحماية البيانات، بدلاً من النهج الحالي المجزأ على مستوى الولايات.
٢. نهج قائم على المخاطر: تبني نهج تنظيمي يركز على المخاطر، حيث تخضع الممارسات عالية المخاطر لقيود أكثر صرامة.
٣. قيود على جمع البيانات: فرض قيود على كمية ونوع البيانات التي يمكن جمعها، بدلاً من الاعتماد فقط على الموافقة.
٤. المساءلة الخوارزمية: تطوير أطر تنظيمية للخوارزميات وأنظمة الذكاء الاصطناعي المستخدمة في معالجة البيانات الشخصية.
٥. التشغيل البيني: تعزيز قابلية التشغيل البيني بين منصات التواصل الاجتماعي لتقليل تأثيرات الشبكة وتعزيز المنافسة.
٦. تعزيز حقوق المستخدمين الجماعية: توسيع نطاق الحقوق ليشمل الحقوق الجماعية، مثل الحق في عدم الخضوع للتنميط الجماعي.
٧. التعاون الدولي: تعزيز التعاون الدولي في إنفاذ قوانين حماية البيانات عبر الحدود.

وتلعب الهيئات الرقابية والتنظيمية دوراً حاسماً في ضمان الامتثال لتشريعات حماية البيانات، لتعزيز فعالية هذه الهيئات، يمكن اتخاذ الإجراءات التالية:

١. زيادة الموارد: توفير موارد مالية وبشرية كافية للهيئات الرقابية لتمكينها من أداء مهامها بفعالية.
٢. تعزيز الاستقلالية: ضمان استقلالية الهيئات الرقابية عن التأثيرات السياسية والتجارية.
٣. تطوير الخبرات التقنية: بناء القدرات التقنية داخل الهيئات الرقابية لفهم التكنولوجيات المعقدة وتقييمها.
٤. التعاون بين الهيئات: تعزيز التعاون بين هيئات حماية البيانات والهيئات التنظيمية الأخرى، مثل هيئات المنافسة وحماية المستهلك.
٥. المشاركة المجتمعية: إشراك منظمات المجتمع المدني والأكاديميين في عمليات صنع السياسات والرقابة.

في الختام، رغم التقدم المحرز في تشريعات حماية البيانات حول العالم، لا تزال هناك حاجة إلى تطوير أطر تنظيمية أكثر شمولاً وفعالية لمواجهة التحديات المتزايدة للخصوصية في عصر مواقع التواصل الاجتماعي، يتطلب هذا نهجاً متعدد الأبعاد يشمل التشريعات الشاملة، والإنفاذ الفعال، والتعاون الدولي، والمشاركة المجتمعية، تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية

وفي مواجهة التحديات المتزايدة للخصوصية في بيئة مواقع التواصل الاجتماعي، تم تطوير مجموعة متنوعة من الاستراتيجيات والتدخلات التي تهدف إلى مساعدة المستخدمين على حماية خصوصيتهم بشكل أفضل، يمكن تصنيف هذه الاستراتيجيات إلى تدخلات نفسية وسلوكية، واستراتيجيات عملية يمكن للمستخدمين تطبيقها بشكل مباشر.

**تدخلات إثارة الخوف من انتهاك الخصوصية**

تعتمد تدخلات إثارة الخوف (Fear Appeal Interventions) على نظريات علم النفس الاجتماعي التي تشير إلى أن إثارة الخوف من تهديد معين يمكن أن تحفز الأفراد على اتخاذ إجراءات وقائية، في سياق الخصوصية في مواقع التواصل الاجتماعي، تهدف هذه التدخلات إلى زيادة وعي المستخدمين بمخاطر انتهاك الخصوصية وتحفيزهم على تبني سلوكيات أكثر أماناً.

**آلية عمل تدخلات إثارة الخوف**

وفقاً لنظرية حماية الدافع (PMT)، تعمل تدخلات إثارة الخوف من خلال التأثير على تقييمات الأفراد للتهديد (Severity & Vulnerability) وتقييماتهم للاستجابة (Response Efficacy & Self-Efficacy):

١. تقييم التهديد: تهدف التدخلات إلى زيادة إدراك المستخدمين لـ:
- خطورة التهديد (Severity): مدى خطورة العواقب المحتملة لانتهاك الخصوصية (مثل سرقة الهوية، الاحتيال المالي).
- القابلية للتعرض للتهديد (Vulnerability): مدى احتمال تعرض المستخدم شخصياً لانتهاك الخصوصية.

٢. تقييم الاستجابة: تهدف التدخلات إلى زيادة إدراك المستخدمين لـ:

- فعالية الاستجابة (Response Efficacy): مدى فعالية الإجراءات الوقائية الموصى بها في تقليل التهديد.
- الكفاءة الذاتية (Self-Efficacy): مدى ثقة المستخدم في قدرته على تنفيذ الإجراءات الوقائية الموصى بها.

١. عندما يكون تقييم التهديد وتقييم الاستجابة مرتفعين، يزداد دافع المستخدم لحماية خصوصيته وتبني السلوكيات الوقائية.

وقد أظهرت دراسة (Neves et al. ٢٠٢٤) فعالية تدخلات إثارة الخوف من انتهاك الخصوصية في تغيير سلوك المستخدمين، في دراستهم الثانية، قاموا بتعريض مجموعة من المستخدمين لرسائل تثير الخوف بشأن مخاطر الخصوصية في مواقع التواصل الاجتماعي، ووجدوا أن هذه التدخلات أدت إلى تقليل فعلي في استخدام مواقع التواصل الاجتماعي مقارنة بالمجموعة الضابطة.

وخلصوا إلى أن "التدخل المبني على إثارة الخوف من انتهاك الخصوصية هو وسيلة فعالة لمساعدة المستخدمين على تقليل استخدامهم لمواقع التواصل الاجتماعي" (Neves et al., 2024)، هذا يشير إلى أن زيادة وعي المستخدمين بالمخاطر يمكن أن يكون حافزاً قوياً لتغيير السلوك.

**أمثلة عملية لتطبيق هذه التدخلات**

يمكن تطبيق تدخلات إثارة الخوف من خلال عدة طرق:

- حملات التوعية: إطلاق حملات توعية عامة تسلط الضوء على مخاطر انتهاك الخصوصية وتقدم نصائح عملية للحماية.
- الإشعارات داخل التطبيق: عرض رسائل تحذيرية للمستخدمين عند مشاركة معلومات حساسة أو تغيير إعدادات الخصوصية.
- المحتوى التعليمي: إنشاء مقالات ومقاطع فيديو تشرح مخاطر الخصوصية بطريقة واضحة ومقنعة.
- الأدوات التفاعلية: تطوير أدوات تساعد المستخدمين على تقييم مستوى تعرضهم لمخاطر الخصوصية وتقديم توصيات مخصصة.

ومع ذلك، يجب تصميم هذه التدخلات بعناية لتجنب إثارة الخوف المفرط الذي قد يؤدي إلى ردود فعل عكسية، مثل الإنكار أو تجنب المعلومات.

**تاسعاً: دور التركيز التنظيمي في حماية الخصوصية**

كما ذكرنا سابقاً، تشير نظرية التركيز التنظيمي إلى أن الأفراد يختلفون في توجههم نحو تحقيق الأهداف (التركيز الترويجي) أو تجنب المخاطر (التركيز الوقائي)، يمكن استخدام هذه السمة النفسية لتطوير استراتيجيات حماية خصوصية مخصصة.

الأفراد ذوو التركيز الترويجي (Promotion–focus): يركزون على المكاسب المحتملة والطموحات، في سياق الخصوصية، قد يكونون أكثر اهتماماً بفوائد المشاركة الاجتماعية والتواصل، وأقل حساسية لمخاطر الخصوصية.

- الأفراد ذوو التركيز الوقائي (Prevention–focus): يركزون على تجنب الخسائر المحتملة والالتزام بالواجبات، في سياق الخصوصية، قد يكونون أكثر قلقاً بشأن مخاطر انتهاك الخصوصية وأكثر استعداداً لاتخاذ إجراءات وقائية.

بالإضافة إلى التدخلات النفسية والسلوكية، هناك مجموعة من الاستراتيجيات العملية التي يمكن للمستخدمين تطبيقها بشكل مباشر لحماية خصوصيتهم في مواقع التواصل الاجتماعي:

**إدارة إعدادات الخصوصية في مواقع التواصل الاجتماعي**

- مراجعة وتحديث الإعدادات بانتظام: يجب على المستخدمين مراجعة إعدادات الخصوصية الخاصة بهم بشكل دوري وتحديثها لتعكس تفضيلاتهم الحالية.
- تقييد رؤية المنشورات والمعلومات الشخصية: تحديد من يمكنه رؤية المحتوى والمعلومات الشخصية (الأصدقاء فقط، مجموعات محددة، عام).
- تعطيل ميزات تتبع الموقع: إيقاف تشغيل خدمات الموقع الجغرافي للتطبيقات أو تقييد الوصول إليها عند الضرورة فقط.
- إدارة أذونات التطبيقات: مراجعة الأذونات الممنوحة للتطبيقات والمواقع المرتبطة بحسابات التواصل الاجتماعي وإلغاء الأذونات غير الضرورية.
- التحكم في الإعلانات المستهدفة: استخدام الأدوات المتاحة لتقييد استخدام البيانات الشخصية في الإعلانات المستهدفة.

**٧. الخلاصة والتوصيات**

**٧.١ ملخص النتائج الرئيسية**

يتناول هذا البحث تأثير مواقع التواصل الاجتماعي على الخصوصية الشخصية، وهو موضوع بالغ الأهمية في عصرنا الرقمي، مع انتشار مواقع التواصل الاجتماعي بشكل غير مسبوق وتزايد عدد مستخدميها إلى أكثر

من ٤.٦ مليار شخص حول العالم، أصبحت قضايا الخصوصية تشكل تحدياً كبيراً للأفراد والمجتمعات والمؤسسات التنظيمية.

من خلال تحليل الدراسات الأكاديمية الحديثة والتقارير المتخصصة، توصل البحث إلى عدة نتائج رئيسية:

١- جمع البيانات الواسع النطاق: تقوم منصات التواصل الاجتماعي بجمع كميات هائلة من البيانات الشخصية، سواء كانت بيانات مقدمة طوعاً، أو بيانات سلوكية، أو بيانات مستنتجة، كما أشار تقرير EPIC، "شركات التواصل الاجتماعي تجمع بيانات حساسة عن أنشطة الأفراد واهتماماتهم وخصائصهم الشخصية وآرائهم السياسية وعادات الشراء والسلوكيات عبر الإنترنت" (EPIC, n.d.).

٣. تقنيات التتبع المتطورة: تستخدم منصات التواصل الاجتماعي تقنيات متطورة للتتبع، مثل ملفات تعريف الارتباط، وبصمات المتصفح، والتتبع عبر الأجهزة المختلفة، هذه التقنيات تسمح بتتبع المستخدمين حتى خارج منصات التواصل الاجتماعي.

٤. خروقات البيانات المتكررة: شهدت السنوات الأخيرة العديد من حوادث تسريب البيانات الكبرى، مثل فضيحة كامبريدج أناليتيكا، التي أثرت على ملايين المستخدمين وكشفت عن هشاشة حماية البيانات الشخصية.

٥. ظهور إرهاق الخصوصية: أدت الجهود المستمرة والمرهقة لحماية الخصوصية إلى ظهور ظاهرة "إرهاق الخصوصية"، حيث يشعر المستخدمون بالإرهاق والإحباط والاستسلام، كما أشار Chen et al. (٢٠٢٣)، "يلعب إرهاق الخصوصية دوراً حاجباً، حيث أن زيادة تجارب انتهاك الخصوصية وتكاليف الاستجابة ترفع من إرهاق الخصوصية لدى الأفراد، وهذا الشعور بالإرهاق يقلل بشكل كبير من استعداد الأفراد لحماية خصوصيتهم".

٦. تأثير الإدمان على قرارات الخصوصية: يؤثر إدمان مواقع التواصل الاجتماعي على قدرة المستخدمين على اتخاذ قرارات عقلانية بشأن خصوصيتهم، وفقاً لدراسة Neves et al. (٢٠٢٤)، "إدمان مواقع التواصل الاجتماعي يقلل من تأثير مخاوف الخصوصية على نوايا تقليل الاستخدام".

٧. احتكار المنصات وتأثيره على الخصوصية: أدى تركيز السوق واحتكار منصات التواصل الاجتماعي إلى الحد من خيارات المستخدمين وقدرتهم على التفاوض بشأن شروط الخصوصية، كما أشار تقرير EPIC، "تتفاقم مخاطر الخصوصية للشبكات الاجتماعية من خلال تركيز المنصات، مما مكّن بعض شركات وسائل التواصل الاجتماعي من الاستحواذ على المنافسين وممارسة القوة الاحتكارية والحد بشدة من ظهور بدائل تحمي الخصوصية" (EPIC, n.d.).

٦- التطور التكنولوجي السريع: تتطور التكنولوجيا بوتيرة أسرع من التشريعات، مما يخلق ثغرات تنظيمية للتقنيات الجديدة.

٧- التغطية التشريعية غير المتكافئة: تختلف مستويات حماية البيانات بشكل كبير بين الدول والمناطق، مما يخلق "ملاذات آمنة" للشركات.

٨- صعوبة الإنفاذ: غالباً ما تفتقر السلطات التنظيمية إلى الموارد والخبرات اللازمة لإنفاذ التشريعات بفعالية.

٩- تعقيد إعدادات الخصوصية: غالباً ما تكون إعدادات الخصوصية في مواقع التواصل الاجتماعي معقدة وصعبة الفهم.

١٠- الحاجة إلى توازن: تحقيق التوازن بين الاستفادة من مزايا مواقع التواصل الاجتماعي وحماية الخصوصية الشخصية.

**التوصيات والمقترحات**

في ضوء النتائج التي توصل إليها البحث، يمكن تقديم التوصيات التالية:

١- رفع الوعي بقضايا الخصوصية

٢- التثقيف المستمر: البقاء على اطلاع بأحدث التطورات في مجال الخصوصية الرقمية والتهديدات المحتملة.

٣- فهم سياسات الخصوصية: محاولة قراءة وفهم سياسات الخصوصية للمنصات المستخدمة، أو على الأقل الأجزاء الأكثر أهمية منها.

٤- الوعي بقيمة البيانات الشخصية: إدراك أن البيانات الشخصية هي عملة في الاقتصاد الرقمي، وأن "الخدمات المجانية" غالباً ما تكون مدفوعة ببيانات المستخدمين.

٥- متابعة أخبار خروقات البيانات: البقاء على اطلاع بأخبار خروقات البيانات التي قد تؤثر على الحسابات الشخصية.

٦- مراجعة وتحديث إعدادات الخصوصية بانتظام: تخصيص وقت دوري لمراجعة وتحديث إعدادات الخصوصية في جميع المنصات المستخدمة.

٧- استخدام كلمات مرور قوية وفريدة: استخدام كلمات مرور قوية ومختلفة لكل حساب، والاستعانة بمديري كلمات المرور.

٨- تفعيل المصادقة الثنائية: تفعيل المصادقة الثنائية لجميع الحسابات التي تدعم هذه الميزة.

٩- التفكير قبل النشر: التفكير في العواقب المحتملة لمشاركة معلومات معينة قبل نشرها.

١٠-الحذر من التطبيقات والاختبارات: توخي الحذر عند استخدام تطبيقات الطرف الثالث واختبارات الشخصية التي تطلب الوصول إلى البيانات الشخصية.

١١-استخدام أدوات حماية الخصوصية: الاستفادة من أدوات حماية الخصوصية مثل متصفحات تركز على الخصوصية، وإضافات حظر التتبع، وشبكات VPN.

١٢-تحديد حدود واضحة: تحديد ما هي المعلومات التي يمكن مشاركتها وما هي المعلومات التي يجب الاحتفاظ بها خاصة.

١٣-إدارة الوقت المستخدم: وضع حدود زمنية لاستخدام مواقع التواصل الاجتماعي لتجنب الإدمان وتقليل التعرض لمخاطر الخصوصية.

١٤-تنويع المنصات المستخدمة: عدم الاعتماد على منصة واحدة، واستكشاف منصات بديلة تقدم ضمانات أفضل للخصوصية.

١٥-أخذ "إجازات رقمية" دورية: تخصيص فترات للابتعاد عن مواقع التواصل الاجتماعي لإعادة تقييم العلاقة معها.

١٦-تثقيف الأسرة والأصدقاء: نشر الوعي بقضايا الخصوصية بين الأسرة والأصدقاء، خاصة الأطفال والمراهقين.

١٧-تبسيط سياسات الخصوصية: تقديم سياسات خصوصية واضحة وسهلة الفهم، مع تجنب اللغة القانونية المعقدة.

١٨-استخدام الملخصات والرسوم البيانية: تقديم ملخصات مرئية وموجزة للنقاط الرئيسية في سياسات الخصوصية.

١٩-الإخطار الفعال بالتغييرات: إخطار المستخدمين بشكل واضح وفعال عند إجراء تغييرات على سياسات الخصوصية.

٢٠-توفير خيارات حقيقية: منح المستخدمين خيارات حقيقية فيما يتعلق بجمع واستخدام بياناتهم، بدلاً من نهج "الموافقة أو المغادرة".

٢١-دمج الخصوصية في عملية التصميم: تضمين اعتبارات الخصوصية في جميع مراحل تطوير المنتجات والخدمات.

٢٢-الإعدادات الافتراضية الآمنة: جعل إعدادات الخصوصية الأكثر أماناً هي الإعدادات الافتراضية.

٢٣-تقليل جمع البيانات: جمع الحد الأدنى من البيانات الضرورية لتقديم الخدمة.

٢٤-تعزيز الشفافية: توفير معلومات واضحة حول كيفية جمع البيانات واستخدامها ومشاركتها.

٢٥-تمكين المستخدمين: توفير أدوات سهلة الاستخدام للمستخدمين للتحكم في بياناتهم.

**٧.٤ آفاق البحث المستقبلية**

في ضوء النتائج والتوصيات، يمكن اقتراح عدة مجالات للبحث المستقبلي:

**مجالات بحثية مقترحة**

١. تطوير وتقييم تدخلات فعالة لمكافحة إرهاق الخصوصية: دراسة كيفية تصميم تدخلات فعالة لمساعدة المستخدمين على التغلب على إرهاق الخصوصية.
٢. استكشاف تأثير الفروق الفردية على سلوكيات الخصوصية: دراسة كيف تؤثر العوامل الشخصية، مثل التركيز التنظيمي والسمات الشخصية، على سلوكيات الخصوصية.
٣. تقييم فعالية التشريعات الحالية: دراسة تأثير التشريعات مثل GDPR وCCPA على ممارسات الخصوصية في مواقع التواصل الاجتماعي.
٤. تطوير نماذج جديدة للموافقة المستنيرة: استكشاف بدائل لنموذج الموافقة الحالي، الذي أثبت محدوديته في سياق مواقع التواصل الاجتماعي.
٥. دراسة تأثير الذكاء الاصطناعي على الخصوصية: استكشاف كيف يمكن للتطورات في الذكاء الاصطناعي أن تؤثر على الخصوصية في مواقع التواصل الاجتماعي.

**تحديات بحثية مستقبلية**

١. التطور السريع للتكنولوجيا: يشكل التطور السريع للتكنولوجيا تحدياً للباحثين، حيث قد تصبح النتائج قديمة بسرعة.
٢. صعوبة الوصول إلى البيانات: قد يكون من الصعب الوصول إلى بيانات دقيقة حول ممارسات جمع البيانات في منصات التواصل الاجتماعي.
٣. تعقيد قياس السلوك الفعلي: غالباً ما يكون هناك فجوة بين النوايا المعلنة والسلوك الفعلي فيما يتعلق بالخصوصية.
٤. الاختلافات الثقافية والجغرافية: تختلف مفاهيم وتوقعات الخصوصية بشكل كبير بين الثقافات والمناطق المختلفة.

**قائمة المراجع**

**المصادر الأكاديمية**

1. Chen, Y., Yan, F., Zahedi, F. M., & Abbasi, A. (2023). Breaking the vicious cycle of privacy fatigue: How regulatory focus moderates the effect of privacy violation experiences and response costs on privacy fatigue. Information Systems Research, 34(1), 67-85. https://doi.org/10.1287/isre.2022.1133
2. Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42-51. https://doi.org/10.1016/j.chb.2017.12.001

3. Neves, A. L. M., Vieira, V. A., & Almeida, S. O. (2024). The role of social media addiction in the relationship between privacy concerns and intentions to reduce social media use. Journal of Marketing Communications, 1-22. https://doi.org/10.1080/13527266.2024.2424922
4. Venkatesh, V., Sykes, T. A., Chan, F. K., Thong, J. Y., & Hu, P. J. (2019). Children's Internet addiction, family-to-work conflict, and job outcomes: A study of parent-child dyads. MIS Quarterly, 43(3), 903-927. https://doi.org/10.25300/MISQ/2019/12338
5. York, C., & Turcotte, J. (2015). Vacationing from Facebook: Adoption, temporary discontinuance, and readoption of an innovation. Communication Research Reports, 32(1), 54-62. https://doi.org/10.1080/08824096.2014.989975

**التقارير والمصادر الإلكترونية**

1. Electronic Privacy Information Center (EPIC). (n.d.). Social Media Privacy. https://epic.org/issues/consumer-privacy/social-media-privacy/
2. European Commission. (2018). General Data Protection Regulation (GDPR). https://gdpr.eu/
3. Federal Trade Commission. (2019). FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
4. Pew Research Center. (2023). Social Media Use in 2023. https://www.pewresearch.org/internet/2023/09/28/social-media-use-in-2023/
5. Statista. (2024). Number of social network users worldwide from 2017 to 2027. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

**التشريعات والقوانين**

1. California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq . (2018).
2. California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100 et seq, (2020)

٣. قانون حماية البيانات الشخصية الاتحادي رقم ٤٥ لسنة ٢٠٢١، الإمارات العربية المتحدة.

٤. نظام حماية البيانات الشخصية، المملكة العربية السعودية (٢٠٢١).

٥. قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، جمهورية مصر العربية.

٦. قانون حماية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦، دولة قطر.

٧. قانون حماية البيانات الشخصية رقم ٣٠ لسنة ٢٠١٨، مملكة البحرين.