الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف بالمسيلة

كلية العلوم الإنسانية والاجتماعية

قسم علوم الإعلام والاتصال

الرقم التسلسلي:. .....

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في

تخصص: اتصال وعلاقات عامة

بعنوان:

تصميم حملة إعلامية لحماية خصوصية مستخدمي شبكات التواصل الاجتماعي

إعداد:

- الطالب: مختاري فيصل

أمام لجنة المناقشـــة المتكونة من السادة الأساتذة:

اسم ولقب الأستاذ	الرتبة	الجامعة	الصفة
د غزال عبد الرزاق	أستاذ محاضر "أ"	جامعة المسيلة	رئيسا
د. بوقرة رضوان	أستاذ محاضر "أ"	جامعة المسيلة	مشرفا ومقررا
د جعفر محمد	أستاذ محاضر "أ"	جامعة المسيلة	مناقشا

السنة الجامعية: (2024-2025) (1445-1446هـ)


بسم الله الرحمن الرحيم

بِسْمِ اللهِ الرَحْمَنِ الرَحِيمْ

{وَ اَللهِ أَخْرَجَكُمْ مِنْ بُطُونِ أُمَهَاتِكُمْ لا تَعْلَمُونَ شَيْئا ًوَجَعَلَ لَكُمْ السَّمْعَ وَالأَبْصَارَ وَالأَفْئِدَةَ لَعَلَكُمْ تَشْكُرُونْ} **(النحل:78)**

شكر وعرفان

قال الله تعالى:

{رَبِ أَوْزِعْنِي أَنَ أَشْكُرَ نِعْمَتَكَ التِي أَنْعَمْتَ عَلَي وَعَلَى وَالِدَيْ وَأَنْ أَعْمَلَ صَالحَاً تَرْاضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَالحِين}النمل الآية 19

أتقدم بخالص الشكر وعظيم الامتنان إلى كل من ساندني ووقف إلى جانبي طيلة مراحل إعداد هذه المذكرة، وعلى رأسهم أسرتي الكريمة التي لم تبخل عليّ بالدعم المعنوي والدعاء الصادق.

كما أخص بالشكر أساتذتي الكرام على ما قدموه لي من توجيه ونصح طيلة رحلتي العلمية ،

ونخص بالذكر أستاذي المشرف " **أ . د . بوقرة رضوان** " الذي كان له الفضل في الاشراف على إنجاز هذا العمل المتواضع جيث لم يبخل علينا بنصائحه وتوجيهاته طيلة الدراسة.

وأسأل الله أن يوفقني لما فيه الخير، وأن يجعل هذا الجهد نافعا، وأن يكلل مساعي جميع الطلبة بالنجاح والتوفيق.

الطالب: مختاري فيصل

إهداء:

إلى من غرَس فيّ حب العلم، وكان سندي في كل مراحل حياتي...

إلى والديّ العزيزين، رمز التضحية والعطاء، شكرًا من القلب على دعمكما اللامحدود.

إلى إخوتي وأخواتي، شركاء الدرب والمحفّزين دومًا،

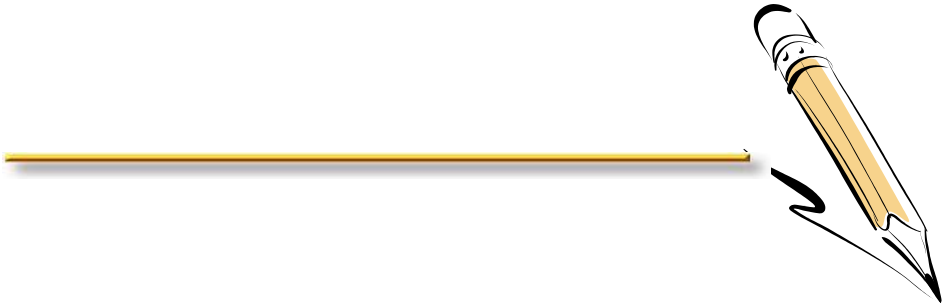
إلى كل من آمن بي وشجعني بكلمة أو دعاء...

أُهدي هذا العمل المتواضع عربونَ وفاء وتقدير، راجيًا من الله أن يكون خطوة أولى في درب النجاح والعطاء.

المهدي: مختاري فيصل

فهرس المحتويات

فهرس المحتويات:



مقدمة

مقدمة:

شهد القرن الحادي والعشرون ثورة رقمية غير مسبوقة مست جميع جوانب الحياة، حيث أصبحت التقنيات المعلوماتية والرقمية حجر الأساس في مختلف القطاعات. فقد بات الاعتماد على الإنترنت جزءًا لا يتجزأ من الحياة اليومية للأفراد والمؤسسات على حد سواء، نظرًا لما توفره من خدمات إلكترونية تختصر الجهد والوقت، وتزيد من سرعة الوصول إلى المعلومات والاتصال.

وقد كان لهذا التحول الرقمي أثر بالغ في ميدان الإعلام والاتصال، حيث ظهرت أنماط جديدة من التواصل، على رأسها شبكات التواصل الاجتماعي التي أفرزتها خدمات الجيل الثاني للويب. فقد شكلت هذه الشبكات، مثل فيسبوك وتويتر ويوتيوب وغيرها، أدوات تواصلية فعالة فتحت المجال أمام المستخدمين للتعبير عن آرائهم وتبادل المعلومات والتفاعل في فضاء افتراضي يختزل الزمان والمكان، ويكسر الحواجز النفسية والثقافية. وتعتبر هذه المنصات اليوم من أبرز مظاهر الإعلام الجديد الذي أعاد تشكيل العلاقات الاجتماعية، وفرض تحولات عميقة في أساليب التفاعل المجتمعي.

إلا أن هذه الثورة الرقمية، ورغم ما تحمله من إيجابيات، أفرزت العديد من التحديات والمخاطر، كان أبرزها التهديدات المتعلقة بحماية البيانات الشخصية، حيث لم تعد الخصوصية أمرًا مضمونًا في ظل الانفتاح غير المسبوق وتدفق البيانات. فقد أصبح ما يُنشر عبر منصات التواصل الاجتماعي متاحًا للعامة، مما جعل الأفراد عرضة لانتهاكات تمس حياتهم الخاصة وكرامتهم، وتحول الفضاء الرقمي في كثير من الأحيان إلى ساحة لانتهاك الحريات بدلًا من تعزيزها.

وتجدر الإشارة إلى أن فئة الشباب تُعد من أكثر الفئات استخدامًا لهذه المنصات، نظرًا لما توفره من فرص للتعبير والترفيه وتبادل المعرفة، إلا أن هذا الاستخدام المكثف لا يخلو من مخاطر، خاصة في ظل غياب الوعي الكافي بأساليب حماية الخصوصية

ومواجهة التهديدات الرقمية. وهو ما يدفع بالضرورة إلى التفكير في وسائل توعوية فعالة لتعزيز الوعي الأمني والرقمي لدى المستخدمين.

وقد تناولنا في الجانب المنهجي للدراسة، أهداف الدراسة، الأسباب الذاتية والموضوعية لاختيار الموضوع، مرورا بأهمية الدراسة والمفاهيم والمصطلحات، المنهج المتبع للدراسة، الدراسات السابقة للاستفادة منها.

أما الجانب النظري فتناولنا في الفصل الأول ماهية الحملات الإعلامية، أما الفصل الثاني فكان تحت عنوان شبكات التواصل الاجتماعي وحماية خصوصية المستخدمين وتضمن في المبحث الأول شبكات التواصل الاجتماعي، أما المبحث الثاني فتناول أشكال الانتهاكات وآليات حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي وفي الفصل الثالث الذي يمثل جانبا تطبيقيا للعمل، تطرقنا فيه إلى مراحل تصميم الحملة الإعلامية، بدء بمرحلة ما قبل التصميم ثم مرحلة التصميم، وفي الأخير مرحلة ما بعد التصميم.

الفصل الأول:

الإطار المنهجي للدراسة

1. الإطار المنهجي للدراسة.

1.1. تحديد الإشكالية:

شهد العالم تحوّلًا جذريًا في أنماط التواصل والتفاعل الإنساني مع ظهور شبكات التواصل الاجتماعي، التي أصبحت جزءًا لا يتجزأ من الحياة اليومية. ورغم ما توفره من مزايا كحرية التعبير، وسهولة التواصل، وسرعة الوصول إلى المعلومات، إلا أنها أثارت تحديات جدّية، أبرزها المساس بالخصوصية. فالخصوصية تُعد من الحقوق الأساسية التي تضمن كرامة الإنسان، وقد صانتها مختلف الديانات السماوية والتشريعات الدولية.

غير أن هذه الشبكات، بما توفره من إمكانيات فنية كالتخفي، واستخدام أسماء مستعارة، وانعدام الرقابة الصارمة، جعلت من مسألة حماية الخصوصية معضلة حقيقية أمام الدول والمجتمعات. إذ بات من السهل اختراق البيانات الشخصية، والتجسس على الحياة الخاصة، ونشر المعلومات الحساسة دون إذن أصحابها.

وفي المقابل، يساهم بعض المستخدمين طوعًا في كشف خصوصياتهم عبر مشاركة يومياتهم ومعلوماتهم الشخصية بمحض إرادتهم، ما يعقد المشهد ويجعل من الصعب رسم حدود واضحة بين ما يجب حمايته وما يُعتبر مكشوفًا بموافقة صاحبه. وهنا تظهر الحاجة الملحّة لإيجاد توازن دقيق بين حرية الاستخدام، وضرورة حماية الخصوصية كقيمة إنسانية وقانونية لا يجوز التهاون بها.

وتهدف دراستنا هذه إلى:

- التعريف بمفهوم حماية الخصوصية لدى مستخدمي شبكات التواصل الاجتماعي.
- التعريف بأهمية الخصوصية لدى مستخدمي شبكات التواصل الاجتماعي.
- معرفة مدى التحكم في الخصوصية لدى مستخدمي شبكات التواصل الاجتماعي.
- المساهمة في خلق وتطوير الوعي الجماعي بشأن الظاهرة، فهي سلاح ذو حدين.
- التعرف على طرق تفعيل سياسة الخصوصية على شبكات التواصل الاجتماعي، ومدى دقتها في حماية البيانات.

2.1. أهمية الدراسة:

تتمثل أهمية دراستنا في:

- أهمية الخصوصية، خاصة في ظل انتشار الجرائم الإلكترونية التي انتشرت بفعل التطور التكنولوجي.
- أهمية مواقع شبكات التواصل، كمنصات اجتماعية زادت من التواصل والانفتاح على الآخر، وازداد مع استخدامها عرضا الذات للأفراد، وتراجع هامش الخصوصية.
- انتشار ظاهرة استغلال مواقع شبكات التواصل الاجتماعي في تتبع وكشف خصوصيات الأفراد.

3.1. أسباب اختيار الموضوع:

أ ـ أسباب ذاتية:

- تم اختيارنا لهذا الموضوع بحكم الاهتمام الشخصي وإشباع الفضول الذاتي انطلاقا مما هو ملاحظ اليوم وكذا مواكبة التطورات والتغيرات التي حدثت في الآونة الأخيرة، والرغبة الملحة في تسليط الضوء على واقع الحياة الخاصة في ظل استخدام شبكات التواصل الاجتماعي ومدى تأثير هذه المواقع على خصوصية الأفراد المستخدمين لها.
- الضرورة الذاتية باعتبارنا نتعرض لهذه الأفعال والجرائم بشكل متكرر باعتبارنا مستخدمين لشبكات التواصل الاجتماعي.

ب. أسباب موضوعية: من أهم أسباب ودوافع اختيارنا لهذا الموضوع دون غيره ما يلي:

1- الانتشار الكبير لشبكات التواصل الاجتماعي وتضاعف عدد مشتركيها،

2-أهمية موضوع الخصوصية والحق في حمايتها من الغير.

3-التعرف على الأسباب والدوافع التي تدفع الأفراد لكشف حياتهم الخاصة على شبكات التواصل الاجتماعي.

4- معرفة أنواع الانتهاكات وطرق التعامل معها، والآثار التي تسببها.

5-حاجة مستخدمي شبكات التواصل الاجتماعي لمعرفة حدود الحياة الخاصة عبر شبكات التواصل الاجتماعي

6- قلة وعي مستخدمي شبكة الانترنيت بآليات وسبل مواجهة انتهاكات الخصوصية الرقمية التي يتعرضون لها.

4.1. تحديد المفاهيم والمصطلحات:

- **الحماية لغة:** ورد في المعاجم العربية بيان أصل كلمة حماية؛ فهي: اسم من الفعل حَمَى،

ومنها: " يَحَمِي، احْمِ، حَمْيا وحِمِايةً، فهو حامٍ، والمفعول مَحَمِيّ. (عمر، 1429، ص 568) << وحِمِى أي >> شيء يدافع عنه ويحظر الاقتراب منه (عمر، 1429، ص 569) <<، وأَحْمْى المكان أي >> جَعَلَهُ حِمًى لَا يُقْرَبُ (الزبيدي، ص 478). <<وحَمَى فلان الشيء، أي>> نصره ودافع عنه. "

وتأتي حِمِاية بمعنى: مَنعَه، " أي عزَّة وقوّة وحصانة " (عمر، 1429، ص 2129)

ويتبين من المعاني السابقة، أن الحماية دلالة على الحفظ والصيانة، والمنع والحَصانة؛ التي يتمتع بها شخصٌ أو شيء أو جهةٌ معينة.

- **الحماية اصطلاحًا:**

أما في ترجمان الحماية أنها اسم مشتق من (protecteur) أي حامٍ، مأخوذ عن الكلمة اللاتينية، protector إذ تأتي بمعنى: مدافع أو حارس خاص، وبشكل عام يُقصد بها وسائل تهدف إلى الدفاع عن حق. (كورنو، 1418، ص 727)

ويقصد بالحماية أنها دلالة على: «منع الأشخاص من الاعتداء على حقوق بعضهم البعض بموجب أحكام قواعد قانونية ".

أما منظمة أوكسفام (منظمة عالمية ذات اتحاد دولي، تُعنى بحقوق الإنسان.) فقد عرفت الحماية بأنها: «كافة النشاطات الهادفة إلى الحصول على الاحترام الكامل لحقوق كافة الأفراد دون أي تمييز وفقاً لما تتضمنه القوانين والأطر ذات العلاقة".

ويمكن القول بأن المقصود بالحماية: الوقاية من المخاطر، وذلك من خلال صون المصالح وحفظها والدفاع عنها، وضمان سلامتها من الأفعال غير المشروعة.

- **الخصوصية:**

لغة:

أصل كلمة خصوصية من خصه بالشيء يخصه خصا وخصوصا وخصوصية وخصوصية، وفتح الخاء أفصح. (المصري، 2003 م، ص 27) وقولهم إنما يفعل هذا خصان من الناس أي خواص منهم، واختصه بكذا، أي خصه به، (المصري، 2003 م، ص 27) وخصصي وخصصه واختصه: أفراده به دون غيره والخاصة خلاف العامة، والخاصة من تخصه نفسك أو الذي اختصصته لنفسك. (أحمد،، .سنة 1424 هـ 2003 م، ص 413)

إن وضع تعريف دقيق وجلي للخصوصية يصطلح عليه يعد أمرا عسيرا وصعبا، وهذا ما يظهر في كثير من التشريعات، رغم الاعتراف بهذا الحق. كما تظهر نفس الصعوبة في تحديد المفهوم في الفقه الوضعي والقضاء (قايد، ص 70)، دون التطرق لجزيئات الخلاف الواسع في الفقه حول مدلول الخصوصية أو الحياة الخاصة لما تمتاز به هذه الفكرة من مرونة لا حدود لها ثابتة أو مستقرة من جهة، كما أنها تختلف باختلاف العصور والتقاليد والثقافة والقيم الدينية السائدة والنظام السياسي في كل مجتمع من جهة أخرى.

كما عرفها معهد القانون الأمريكي من زاوية المساس بها قائلا: "كل شخص ينتهك بصورة جدية، وبدون وجه حق شخص أخر، يكون مسؤولا أمام المعتدي عليه وليس من الشك أن هذا معيار واسع، إذا لا يمكن حصر صور الاعتداء بأي حال من الأحوال. (بحر، سنة 1403 هـ،. 1983 م،ص 185)

إن الخصوصية هي حالة ترتبط بالشخص أكثر من المكان، فالمهم هي الحالة التي يكون عليها الشخص لكي يتمتع بالحماية القانونية، وهو ما ذهب إليه المشرع الجزائري حيث بين أن لخصوصية مرتبطة بالوقائع والتصرفات من خلال المادة 24 من المرسوم التشريعي

المتعلق بالمنظومة الإحصائية. (المرسوم التشريعي رقم 01/94 ، المؤرخ في 15 جانفي 1994 ، المنشور في الجريدة الرسمية العدد 03 ، المؤرخة في 16 جانفي1994 ، السنة 31 المتعلقة بالمنظومة الاحصائية).

وتعني الحفاظ على البيانات الشخصية من الاستخدام غير المخول مثل الإضافة والحذف والتعديل.

إجرائيا:

هي أسلوب حياة ومجموعة من أخلاقيات فهي استبعاد الآخرين عن نطاق الحياة واحترام ذاتية الحياة الخاصة من خلال مختلف الصور المتعلقة بانتهاك الخصوصية والمتمثلة في التدخل واستخدام اسم أو صفة الغير معقول وإفشاء الحياة الخاصة وإظهارها بمظهر كاذب للغير.

- **شبكات التواصل الاجتماعي:**

اصطلاحا:

تعرفها "هبة محمد خليفة" بأنها شبكة مواقع فعالة جدا في تسهيل الحياة الاجتماعية بين مجموعة من المعارف والأصدقاء، كما تكمن الأصدقاء القدامى من الاتصال ببعضهم البعض، وتمكنهم أيضا من التواصل المرئي والصوتي وتبادل الصور وغيرها من الإمكانيات التي توطد العلاقة الاجتماعية بينهم. (منصور محمد، 2012، ص 22)

تعرف أيضا على أنها: مواقع على الانترنت يتواصل من خلالها ملايين البشر الذين تجمعهم اهتمامات أو تخصصات معينة ويتاح لأعضاء هذه الشبكات مشاركة الملفات والصور، وتبادل مقاطع الفيديو، وإنشاء المدونات وإرسال الرسائل، وإجراء المحادثات الفورية، وسبب وصف هذه الشبكات بالاجتماعية كونها تتيح التواصل مع الأصدقاء، زملاء الدراسة وتقوي الروابط بين أعضاء هذه الشبكات في فضاء الانترنت.

إجرائيا:

هي مواقع للدردشة وهي عبارة على مواقع الكترونية عبر شبكة الانترنت، تعتبر من أهم الوسائل الاتصالية في وقتنا الحالي، من خلال عملية الاتصال والتواصل ونشر الثقافات عبرها من خلال صور، فيديوهات ومختلف المعلومات والمواضيع.

5.1. الدراسات السابقة:

1. **الدراسة الأولى:** بودربالة عبد القادر 2016 بعنوان "تحديات الخصوصية عبر الفيسبوك: المستخدمون بين حماية الحياة الخاصة وحرية عرض الذات"، حيث تناولت هذه الورقة العلمية إشكالية الخصوصية على منصة فيسبوك، من خلال دراسة التوتر القائم بين رغبة المستخدمين في الحفاظ على خصوصيتهم من جهة، وحرية عرض الذات من جهة أخرى. وقد ركّزت الدراسة على آثار تداخل المجالين الخاص والعام، والمخاطر الناتجة عن الإفراط في عرض الذات على الموقع، في محاولة للكشف عن التحديات التي تواجه الخصوصية الرقمية.

وتمحورت إشكالية الدراسة حول التساؤل التالي :*ما هي أخطار العرض الرقمي للذات عبر الفيسبوك على الخصوصية؟*، وذلك في إطار محاولة لفهم التحول الذي طرأ على مفهوم الخصوصية في العصر الرقمي، من خلال تحديد ممارسات وسلوكيات مستخدمي الفيسبوك، ما دفع الباحث إلى التعمق في تحليل تلك التحديات. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال تحليل مضمون تفاعلات وسلوكيات المستخدمين على منصة فيسبوك.

2. **الدراسة الثانية:** تومي فضيلة (2017) بعنوان "إيديولوجيا الشبكات الاجتماعية وخصوصية المستخدم بين الانتهاك والاختراق"، تهدف هذه الدراسة إلى تسليط الضوء على المخاطر والآثار المرتبطة بعرض الذات على مواقع التواصل الاجتماعي، وتناول التحديات المتعددة التي يواجهها المستخدمون في حماية خصوصياتهم ضمن هذه الفضاءات الافتراضية التي باتت شفافة تماماً، حيث أصبح من المألوف أن تقديم الذات في هذه البيئات

الرقمية يقتضي عرض معلومات وبيانات شخصية حساسة، مما يعرض المستخدم لمخاطر عديدة.

كما تناولت الدراسة مسألة التفكك التدريجي والتقارب بين المجالين العام والخاص، وهو ما أثار إشكالية السيطرة على الخصوصية في بيئة الشبكات. وقد تمحورت إشكالية الدراسة حول التساؤل التالي: هل ستتوقف مواقع التواصل الاجتماعي عند حد انتهاك خصوصية المستخدم فقط، أم أن ذلك جزء من سياسة مدروسة تهدف إلى تنفيذ أيديولوجيا خفية تتبعها الشركات المالكة لهذه المنصات؟ واعتمدت الباحثة على المنهج الوصفي التحليلي لتحليل الظواهر الاجتماعية المرتبطة باستخدام شبكات التواصل الاجتماعي

وتوصلت الدراسة إلى عدة نتائج، أهمها: أن العديد من المستخدمين يظنون أنهم في عصر شبكات التواصل الاجتماعي قد أنشأوا لأنفسهم عالمًا رقميًا يبحرون فيه عبر هويات افتراضية، لكنهم يغفلون أنهم أصبحوا أسرى لهذه الشبكات التي تتحكم في علاقاتهم وسلوكياتهم من خلال فرض شروط الاستخدام واقتراح الأصدقاء. ومع انتشار الشبكات واستحواذها على وقت المستخدمين، حدث نوع من التلاشي للخصوصية الفردية وتجاوز المفهوم التقليدي لها. وفي النهاية، تؤكد الدراسة أن خصوصيات مستخدمي شبكات التواصل الاجتماعي باتت تتآكل بسرعة، متأرجحة بين الانتهاك والاختراق لصالح هذه المنصات ذات الطابع الاقتصادي، والتي تستغل البيانات لأغراض إعلانية وتسويقية وأحيانًا أمنية، مما يفرض على المستخدمين توخي الحذر بشأن ما ينشرونه ويتفاعلون معه على هذه الشبكات.

3. **الدراسة الثالثة:** دراسة الباحث مدور إسماعيل (2019 (بعنوان "واقع الخصوصية الفردية لدى مستخدمي الفيسبوك"، وهي دراسة ميدانية أجريت على عينة من طلبة الماستر تخصص اتصال جماهيري بجامعة قاصدي مرباح – ورقلة، وقد قُدمت كمذكرة لاستكمال متطلبات نيل شهادة الماستر. انطلقت الدراسة من الإشكالية التالية :*ما واقع الخصوصية الفردية لدى مستخدمي الفيسبوك من الطلبة؟*، وقد تم الاعتماد على المنهج الوصفي التحليلي في الجانب النظري من خلال تقديم التعاريف، وضبط المصطلحات والمفاهيم، والتطرق

للمداخل العامة ذات الصلة بأثر الخصوصية الفردية على مستخدمي موقع فيسبوك والعلاقة القائمة بينهما، مستندةً في الجانب التطبيقي على أداة الاستمارة لجمع البيانات من العينة.

وتهدف الدراسة إلى الكشف عن واقع الخصوصية الفردية لدى الطلبة الجامعيين مستخدمي موقع فيسبوك، حيث تم اختيار عينة من طلبة تخصص اتصال جماهيري بكلية العلوم الإنسانية، قسم علوم الإعلام والاتصال. وقد شملت الاستمارة ثلاثة محاور رئيسية: المحور الأول يتناول طبيعة خصوصية مستخدمي الفيسبوك، بينما يركز المحور الثاني على كيفية تعامل المستخدمين مع مستوى الأمان الذي يوفره الموقع، أما المحور الثالث فاهتم بإرشادات حماية الخصوصية والسياسات المعتمدة من قبل إدارة فيسبوك.

4. **الدراسة الرابعة:** دراسة مرزوقي الدراجي سنة 2020 بعنوان تصميم حملة إعلامية حول الوقاية من حرائق الغابات، مذكرة مكملة لنيل شهادة الماستر في علوم الاعلام ولاتصال تخصص اتصال وعلاقات عامة، جامعة محمد بوضياف المسيلة، وكانت إشكالية الدراسة تدور حول الحملات الإعلامية ومدى مساهمتها في الحد من ظاهرة حرائق الغابات باعتبار أن الحملة الإعلامية من بين أهم الوسائل الناجحة في تحقيق ذلك. حيث جاءت أهداف الدراسة على النحو التالي:

1.التوعية و التحسيس بظاهرة خطيرة هي حرائق الغابات.

2.تسليط الضوء على ظاهرة حرائق الغابات وكيفية المحافظة عليها.

3.التعرف على أهم الوسائل ا ولآليات المستخدمة للحد من حرائق الغابات.

4.معرفة مدى أهمية الحملات الإعلامية التوعية في الحد من حرائق الغابات.

تثمين الحملات الإعلامية من خلال البحث العلمي.

وقد اعتمد الإجراءات المنهجية المعمول بها في قسم الإعلام والاتصال وكانت خطة البحث على النحو الآتي :

الإطار العام للدراسة :ويشمل الإشكالية وأسباب اختيار الموضوع وكذا الأهمية والأهداف بالإضافة إلى تحديد مصطلحات الدراسة والدراسات السابقة.

الفصل الثاني :الإطار النظري للدراسة :وشمل أهمية الغابات وخطورة الحرائق ا ولحملات الإعلامية. الفصل الثالث :الإطار التطبيقي. ويحتوي على ثلاث مراحل هي مرحلة ما قبل التصميم ومرحلة التصميم ومرحلة ما بعد التصميم.

التعقيب على الدراسات السابقة:

تُبرز المقارنة بين الدراسات الأربع ودراستنا الموسومة بـ «تصميم حملة إعلامية لحماية خصوصية مستخدمي شبكات التواصل الاجتماعي" أوجه تشابه واختلاف مهمة من حيث الموضوع والمنهج والطرح. إذ تتقاطع الدراسات الثلاث الأولى، وهي دراسة بودربالة عبد القادر (2016)، وتومي فضيلة (2017)، ومدور إسماعيل (2019)، مع دراستنا في تناول موضوع الخصوصية الرقمية ومخاطر انتهاكها في بيئة شبكات التواصل الاجتماعي، سواء من منظور نظري تحليلي أو ميداني. ومع ذلك، تختلف دراستنا من حيث طبيعتها التطبيقية، حيث لم تركز على جمع البيانات وتحليلها إحصائياً كما فعلت الدراسات الثلاث، بل اتجهت نحو تصميم حملة إعلامية توعوية تستهدف فئة الشباب الجامعي، لتقديم حلول اتصالية ملموسة ومحتوى إعلامي يعزز الوعي بسبل حماية الخصوصية.

أما الدراسة الرابعة التي أنجزها مرزوقي الدراجي (2020)، وإن كانت مختلفة موضوعيًا كونها تناولت الوقاية من حرائق الغابات، فإنها تتقاطع مع دراستنا من حيث الشكل والمنهج التطبيقي، حيث اعتمدت بدورها على تصميم حملة إعلامية كوسيلة للتوعية والتوجيه. ومن هذا المنطلق، يمكن اعتبار دراستنا مكملة لسياق الدراسات السابقة، إذ سعت إلى نقل موضوع الخصوصية من دائرة الطرح النظري أو التحليل السلوكي إلى دائرة التفعيل العملي ولاتصالي، من خلال استخدام الحملة الإعلامية كوسيلة فعالة لترسيخ مفاهيم الأمن الرقمي لدى الشباب الجامعي. وعليه، فإن دراستنا تسد فراغًا في الأدبيات المتعلقة بالخصوصية الرقمية، لكونها تقدم نموذجًا تطبيقيًا يربط بين التنظير الإعلامي والعمل الميداني التوعوي، وهو ما يميزها عن بقية الدراسات السابقة في المجال.

الفصل الثاني:

ماهية الحملة الإعلامية

2. ماهية الحملة الإعلامية.

تمهيد:

تشير الحملة الإعلامية إلى مجموعة من الأنشطة الاتصالية المخططة والمنظمة التي تهدف إلى التأثير في الرأي العام أو توجيهه نحو قضية معينة، أو الترويج لفكرة، أو خدمة، أو منتج، باستخدام وسائل الإعلام المختلفة كالتلفزيون، الإذاعة، الصحف، الإنترنت، وشبكات التواصل الاجتماعي.

تُبنى الحملة الإعلامية على استراتيجيات مدروسة تحدد الأهداف، والجمهور المستهدف، والرسائل الأساسية، ووسائل الترويج، والفترة الزمنية للتنفيذ. وقد تكون توعوية، سياسية، اجتماعية، أو تجارية، وتُستخدم في مجالات متعددة مثل الصحة العامة، الانتخابات، الحملات البيئية، أو حتى في إدارة الأزمات.

وتكمن فعالية الحملة الإعلامية في قدرتها على إيصال الرسالة بطريقة جذابة ومقنعة، وتحقيق التفاعل المطلوب من الجمهور، وهو ما يتطلب انسجامًا بين المحتوى الإعلامي والوسائل المستخدمة، إضافة إلى دراسة دقيقة للجمهور المستهدف من حيث ثقافته، اهتماماته، وميولاته.

1.2. مفهوم الحملات الإعلامية:

اختلف الباحثون في تعريف الحملة الإعلامية، وتعددت وجهات نظرهم بشأنها، غير أن هذه التعاريف، على اختلاف صياغاتها، تتفق في مضمونها الجوهري. وفي هذا السياق، نعرض بعض التصورات حول مفهوم الحملة الإعلامية. فقد عرّفها "جاسبر براجت" بأنها مجموعة مترابطة من الرسائل الإعلامية المصممة وفق معايير محددة، تهدف إلى تحقيق غايات واضحة، وذلك من خلال توظيف عدة وسائل إعلامية، والاستعانة بتقنيات متطورة تسهم في تتبع مسار الحملة. كما أكد على ضرورة التنسيق بين مختلف الوسائط الإعلامية لضمان فاعلية البث والوصول الأمثل إلى الجمهور المستهدف وتحقيق أقصى قدر من التأثير. (سليم، 2013، ص 303)

يعرّف صابر سليمان عسران الحملة الإعلامية بأنها "جهود منظمة ينفذها متخصصون في مجال الإعلام باستخدام وسائله المتنوعة، بهدف تحقيق هدف أو مجموعة من الأهداف المسبقة التحديد، تُوجَّه إلى فئة معينة باستخدام لغتها الخاصة، ومن خلال الأطر الثقافية التي تنتمي إليها، وذلك خلال فترة زمنية محددة. وتعتمد هذه الحملة على تحديد دقيق للجمهور المستهدف، واختيار الوسائل الإعلامية الأنسب له بما يضمن فعالية الرسالة الإعلامية وتأثيرها".

- يُعرّف دينيس ماكويل الحملة الإعلامية بأنها "جهود اتصالية مؤقتة تستند إلى سلوك جماعي أو مؤسسي يتماشى مع القيم والمعايير الاجتماعية السائدة، وتهدف إلى توجيه ودعم وتحفيز اتجاهات الجمهور نحو أهداف تحظى بقبول اجتماعي، مثل: المشاركة في التصويت، أو الإقبال على شراء سلع معينة، أو السعي نحو تحقيق مستويات أعلى من الأمن أو الصحة العامة (كنعان، 2014، ص 33)

يعرّف غو ران هدبرو (Hidbrow) الحملة الإعلامية بأنها "نشاط إعلامي مكثف يُنفّذ خلال فترة زمنية محددة، ويتناول موضوعًا بعينه، ويعتمد عادةً على استخدام مجموعة متنوعة من الوسائل الإعلامية لتحقيق أهدافه". (الكافي، 2015 ، ص09)

- يعرّف الدكتور محمود أدهم الحملة الإعلامية بأنها "أسلوب صحفي متميّز يتميّز بقدرته على التأثير في الرأي العام، من خلال سعيه إلى طرح حلول للمشكلات التي تؤرق المجتمع وتُقلق أفراده، ومهاجمة الأوضاع السلبية والدعوة إلى إصلاحها في مختلف الميادين، فضلاً عن دعم وتأييد الأفكار البنّاءة والمضيئة"

يعرّف جلال الدين الحمامصي الحملة الإعلامية بأنها "عمل إعلامي يقوم على المعالجة العميقة والمطوّلة، يهدف من خلالها كاتب الحملة إلى لفت الانتباه إلى وضع معيّن قد يُلحق الضرر ببنية المجتمع، أو إلى حالة تستدعي التغيير الجذري لكونها تتعارض مع مصلحة الجمهور أو الرأي العام". (الكافي، 2015 ، ص15)

تُعرّف الحملة الإعلامية أيضًا بأنها "نشاط اتصالي مخطط ومنظم، يخضع للمتابعة والتقويم، وتقوم به مؤسسات أو مجموعات من الأفراد خلال فترة زمنية محددة، بهدف تحقيق غايات معينة، ويعتمد هذا النشاط على توظيف وسائل الاتصال المتنوعة، من خلال بث سلسلة من الرسائل الاتصالية المدروسة، باستخدام أساليب إقناع واستمالة فعّالة تتناول موضوعًا محددًا، سواء لتأييده أو معارضته، ويُوجَّه إلى جمهور واسع نسبيًا".

انطلاقًا مما سبق، يمكن تعريف الحملة الإعلامية بأنها "مجموعة من الأنشطة والبرامج الاتصالية المخططة والمنظمة، يتم إعدادها وفق معايير محددة سلفًا، بما يتلاءم مع موضوع الحملة وأهدافها الجوهرية. وتهدف هذه الحملات إلى تحقيق التأثير المرجو في أكبر شريحة ممكنة من الجمهور المستهدف، خلال فترة زمنية معينة، وذلك من خلال استخدام وسائل وأدوات إعلامية فعّالة ومتكاملة."

2.2. أنواع الحملات الإعلامية:

- تتفاوت الحملات الإعلامية من حيث الحجم والشكل باختلاف الأهداف والغايات التي تنشد تحقيقها، الأمر الذي يجعل من تصنيفها عملية متعددة الأبعاد. فبينما يميل بعض الباحثين والمتخصصين في علم الاجتماع والعلاقات العامة إلى تصنيف الحملات الإعلامية بناءً على موضوعاتها أو مجالاتها، يعتمد آخرون في تصنيفهم على الأهداف والغايات التي

تسعى الحملة إلى بلوغها. في المقابل، يركّز البعض على الوسائل والأدوات المستخدمة في تنفيذ الحملة ونشر مضامينها. وفي إطار هذه الدراسة، سنتعرض لبعض التصنيفات المعتمدة للحملات الإعلامية وفق المعايير التالية:

- **أولًا: من حيث خدماتها أو غاياتها:**

تختلف أشكال وأحجام الحملات الإعلامية تبعًا لأهدافها، ويتم إعدادها بما يتماشى مع الغاية المنشودة، ومن أبرز أنواع الحملات في هذا السياق:

- حملات تعريفية تهدف إلى تقديم المنظمة، وأهدافها، وأنشطتها وخدماتها للجمهور.
- حملات موجهة لبناء الصورة الذهنية للمنظمة وتعزيز هويتها الإعلامية.
- حملات تسويقية لمنتجات أو خدمات معينة.
- حملات للترويج لأنشطة أو فعاليات محددة مثل المؤتمرات أو الملتقيات.
- حملات توعية ذات طابع صحي أو اجتماعي تستهدف رفع مستوى الوعي لدى الجمهور.
- **ثانيًا: من حيث الوسائل والأدوات المستخدمة:**

تتنوع الحملات الإعلامية كذلك بحسب الوسائل التي تُستخدم في تنفيذها، ومنها:

- الحملة التلفزيونية.
- الحملة الإذاعية.
- الحملة الإلكترونية أو ما يُعرف بالإعلام الجديد.
- الحملة الصحفية.
- الحملة الميدانية المباشرة.
- حملة العلاقات العامة. ((http://www.namaa.com sa/ le 25/03/2019- 18:55))

ثالثا: من حيث أهدافها:

1-**حملات التغيير المعرفي:** تهدف هذه الحملات إلى تزويد الجمهور المستهدف بمعلومات محددة أو تعزيز وعيهم بقضية معينة، بالإضافة إلى تصحيح المفاهيم أو المعلومات الخاطئة المنتشرة لديهم. وتقتصر هذه الحملات غالبًا على نقل معلومات هادفة بدون السعي إلى تغيير السلوكيات أو القناعات الشخصية للأفراد، مما يجعلها من أبسط أنواع الحملات الإعلامية من حيث التنفيذ والأهداف، إذ تركز بشكل رئيسي على زيادة مستوى المعرفة فقط دون استهداف التحول السلوكي. (سفيان، 2016، ص 152.)

2-**حملات التغيير السلوكي:** تُعرف هذه الحملات أيضًا باسم الحملات السلوكية، وتهدف إلى تشجيع الأفراد على تعديل بعض أنماط سلوكهم. وتُعد من أصعب أنواع الحملات الإعلامية نظرًا للصعوبات المرتبطة بتغيير العادات الراسخة التي يمارسها الأفراد لفترات طويلة. لتحقيق النجاح، يتعين تمكين المستهدفين من التخلي عن السلوكيات القديمة وتبني عادات جديدة مع الاستمرار في ممارستها. وغالبًا ما تكون وسائل الإعلام الجماهيري وحدها غير كافية لتحقيق هذا التغيير، لذا يُستحسن دعمها بوسائل أخرى مثل اللقاءات المباشرة والتواصل الشخصي لتعزيز التأثير وتحفيز المشاركة. ومن أبرز الأمثلة على هذه الحملات، الحملات التي تشجع على الإقلاع عن التدخين أو تحسين العادات الغذائية. كما تتطلب حملات التوعية المرورية الصبر والاستمرارية لتثبيت السلوكيات الجديدة من خلال توفير الدعم المستمر وحشد الجهود.

3-**حملات التغيير في الفعل (العمل):** يهدف هذا النوع من الحملات إلى حث أكبر عدد ممكن من الأفراد على القيام بفعل معين خلال فترة زمنية محددة. وتكمن التحديات في هذا النوع من الحملات في أن تنفيذ الفعل قد يتطلب من الجمهور بذل جهد، أو تخصيص وقت، أو حتى إنفاق مال، مما قد يؤثر سلبًا على دوافعهم للمشاركة. لذا،

يجب على القائمين على هذه الحملات توفير حوافز ووسائل داعمة تسهل على الأفراد اتخاذ الخطوة المطلوبة، وتعزز من استجابتهم الإيجابية تجاه الدعوة إلى العمل. (محمد ع.، ص 153. 2012)

4- **حملات التغيير في المعتقدات:** تُعتبر المعتقدات من أقوى ما يؤمن به الإنسان، حيث تمثل إطارًا مرجعيًا وروحيًا قد ينبثق من الدين أو الإيديولوجيا أو العادات والتقاليد الاجتماعية الراسخة في الذاكرة الجماعية، وتلعب الأسرة الدور الأبرز في عملية ترسيخ هذه المعتقدات. إن تغيير المعتقدات الخاطئة يُعدّ من أصعب أشكال التغيير الاجتماعي، نظرًا لأنها نتاج تراكم مئات السنين من التلقين والترسيخ، ويتجذر تأثيرها في سلوكيات الأفراد بشكل عميق، خاصة حينما تستند إلى سند ديني أو عرفي. لذا، تتطلب معالجة هذه القضايا في المقام الأول التعاون مع القادة الروحيين والاجتماعيين، الذين يُعتبرون ممثلين لجماهيرهم وقادة رأي فاعلين، بحيث يقومون بدور محوري في تحويل التأثيرات السلبية لهذه المعتقدات إلى قيم إيجابية تخدم مصلحة المجتمع .

رابعا: من حيث وظيفتها:

1- **الحملات الإخبارية:** تهدف هذه الحملات إلى نقل المعلومات الدقيقة والحقائق الموضوعية إلى الجمهور، من خلال تقديم بيانات موثوقة تتعلق بموضوع الحملة، مما يساهم في إطلاع الجمهور على الوقائع والمستجدات بشكل واضح وشفاف.

2- **حملات الصورة الذهنية** :تركز هذه الحملات على بناء وتعزيز صورة ذهنية إيجابية عن جهة أو مؤسسة أو قضية معينة، وذلك من خلال ترسيخ تلك الصورة في أذهان المتلقين عبر وسائل وأساليب مدروسة تعزز الانطباع المطلوب.

3- **الحملات التعليمية** :تُستخدم هذه الحملات بشكل واسع خاصة أثناء الكوارث والأزمات، حيث تهدف إلى توعية الجمهور وتعليمه كيفية التصرف السليم والمناسب في مثل هذه الظروف الطارئة، لضمان سلامتهم وحماية المجتمع.

4- **الحملات الإقناعية:** تُعتبر من أصعب أنواع الحملات، إذ تتطلب تخطيطًا وتصميمًا وتنفيذًا دقيقًا. تهدف هذه الحملات إلى زرع اتجاهات جديدة في أذهان الجمهور أو تعديل اتجاهات قائمة، مما يستدعي استراتيجيات متقنة للتأثير على المواقف والسلوكيات. (عبير، 2012، ص 96)

5- **الحملات المعلوماتية:** هي حملة معلومات عامة تسعى وراء معرفة الجمهور، وإدراكه لحدث ما، وتزويده ببعض المعلومات العامة الحيوية.

6- **الحملات التربوية:** هي حملة للتعلم، تذهب بخطوة إضافية خلف الوعي والمعلومات إلى التفسير ومقدرة الجمهور على تطبيق المعلومات وتحويلها إلى سلوك يومي.

7- **الحملات الأمنية** :تهدف هذه الحملات إلى رفع مستوى الوعي الأمني لدى الجمهور حول المخاطر والتهديدات المتنوعة التي قد تواجه المجتمع، مع التركيز على متابعة ورصد الأنشطة المشبوهة المتعلقة بالإرهاب والجريمة المنظمة، بهدف تعزيز الأمن والاستقرار.

8- **الحملات الانتخابية** :تُعدّ هذه الحملات دورية وتتركز في الفترات التي تسبق الانتخابات، حيث تعمل على إيصال الرسائل السياسية للمرشحين وبرامجهم الانتخابية إلى الناخبين، بهدف حشد الدعم وضمان الفوز في الانتخابات.

9- **حملات الحرب الدعائية** :تُستخدم هذه الحملات خلال فترات الحروب والنزاعات المسلحة، وتهدف إلى التأثير على معنويات المجتمعات المستهدفة، وزرع الشعور بالانكسار والرغبة في الاستسلام للطرف الخصم، عبر رسائل نفسية وإعلامية مدروسة.

10- **حملات الدعاية المضادة** :يُنفذ هذا النوع من الحملات بهدف مواجهة ومعالجة الدعاية المعادية أو المضادة التي تستهدف المجتمع، حيث تسعى إلى خلق حالة من التوازن الفكري والمعلوماتي والنفسي، مما يساعد في الوقاية من التأثيرات السلبية للدعاية المضادة.

11- **الحملات الإعلامية العسكرية** :تُستخدم هذه الحملات لأغراض الردع الخارجي، وتعزيز ثقة الجمهور في قدرات القوات المسلحة الوطنية. كما تشمل الحملات التغطية الإعلامية للحروب والعمليات العسكرية، بهدف دعم الروح المعنوية وتأمين الدعم الشعبي . (محمد، 2008، ص 45.)

12- **الحملات الإعلامية الخاصة:** وتقوم بها جماعات وأفراد لأهداف مختلفة.

3.2. أهمية وأهداف الحملات الإعلامية:

1- أهمية الحملات الاعلامية:

أظهرت العديد من الدراسات والخبرات المتراكمة فعالية الحملات الإعلامية في تحقيق الأهداف المرجوة وإحداث التأثير المطلوب على الجمهور. كما تلعب هذه الحملات دورًا مهمًا في عملية الإقناع والتغيير الاجتماعي. ومع ذلك، فإن نجاح الحملات الإعلامية يتوقف بشكل أساسي على التخطيط الدقيق، والالتزام بالمبادئ والأسس العلمية الصحيحة، وتطبيق الخطوات العملية المنهجية اللازمة لضمان تحقيق النتائج المرجوة. وإلا، فقد تواجه هذه الحملات تحديات وصعوبات كبيرة قد تعيق تحقيق أهدافها المنشودة. (زهير، 2014، ص99)

تُعتبر الحملات الإعلامية جهدًا منظمًا يهدف إلى إقناع الفئات المستهدفة بأفكار أو اتجاهات أو سلوكيات محددة، أو تعديلها، أو التخلي عنها، ويتم تنفيذها بواسطة جهات أو مجموعات داخل المجتمع، معتمدين على مراحل متتابعة وتأثير تراكمي لضمان تحقيق نتائج ملموسة ومستدامة.

في العصر الحديث، أصبحت الحملات الإعلامية التي ينظمها المختصون في مجال الاتصال ضرورة ملحة، إذ تهدف إلى رفع مستوى الوعي العام وتعزيز مشاركة الجماهير في العملية التنموية التي تقوم بها مختلف المؤسسات. كما تسهم هذه الحملات في التعريف بالإنجازات وتعزيز الثقة بين المؤسسات والجمهور، فضلاً عن رفع المستوى الثقافي للمجتمع، ما يسهم في تقبل الأفكار والسلوكيات الحديثة وتسريع وتيرة التنمية الاجتماعية.

تزداد أهمية الحملات الإعلامية بشكل خاص في ظل وجود فجوات حضارية داخل المجتمعات، حيث يؤدي التطور غير المتوازن إلى تحديات اجتماعية وثقافية متعددة. فبينما يمكن تحقيق التطور المادي بسرعة عبر التعاقد مع شركات كبرى لإنجاز المشاريع خلال فترات زمنية قصيرة، فإن التطور المعنوي، الذي يتجسد في رفع الوعي الثقافي والاجتماعي، يتطلب جهودًا طويلة الأمد تمتد لسنوات عبر التعليم، وبرامج التوعية، ووسائل الإعلام المختلفة. لهذا السبب، لجأت العديد من الدول إلى الاعتماد على الحملات الإعلامية كوسيلة فعالة لتقليص الفجوة الحضارية وتحقيق توازن مستدام بين التطور المادي والثقافي. (زهير، 2014، ص99)

2- أهداف الحملات الإعلامية:

تتضمن الحملات الإعلامية مجموعة متنوعة من الأنشطة المشروعة التي تتباين أهدافها حسب طبيعة النشاط الموجهة نحوه. ويمكن تلخيص الأهداف العامة التي تسعى الحملات الإعلامية الاجتماعية إلى تحقيقها كما يلي:

1. **توفير المعلومات:** تهدف إلى تزويد الفئات المستهدفة بالبيانات والمعلومات المتعلقة بالقضايا التي تؤثر على حياتهم اليومية، بهدف تحفيزهم على إجراء التعديلات اللازمة والمطلوبة.
2. **التأثير على المواقف والاتجاهات:** تسعى هذه الحملات إلى تشكيل آراء الجمهور المستهدف تجاه قضايا محددة أو عامة، بهدف بناء توجهات إيجابية أو تعديل اتجاهات قائمة.
3. **تغيير السلوك أو تعديله:** تركز الحملات على تعديل السلوكيات غير المرغوب فيها من خلال توعية الأفراد بمخاطرها، أو تخفيفها عندما يكون التغيير الكامل صعب التحقيق، مثل حملات السلامة لمرتادي البحر التي تروج لإجراءات السلامة بدلًا من منع السباحة كليًا.

4. **توضيح العواقب:** تهدف بعض الحملات إلى إبراز العواقب الجسدية والنفسية والاجتماعية الناتجة عن ظواهر معينة، مثل التوعية بمخاطر حوادث المرور وتأثيرها السلبي على الأفراد والمجتمع.
5. **تعزيز الوعي الاجتماعي:** تسعى إلى توضيح الحقائق وتعريف المواطنين بحقوقهم وواجباتهم، مثل حملات التوعية بقوانين المرور وأهمية الالتزام بالإشارات وتقليل السرعة.
6. **تحسين صورة المؤسسة وتعزيز الأداء التجاري:** يمكن أن تؤدي الحملة الإعلامية إلى بناء صورة قوية للمؤسسة، مما يسهم في زيادة المبيعات وتحسين الأرباح.
7. تعمل الحملات الإعلامية على التنبيه إلى مخاطر الآفات الاجتماعية وتسليط الضوء على أضرارها، مما يجعلها دعامة أساسية وركيزة هامة لخلق أرضية مشتركة لتبادل المفاهيم والقيم داخل المجتمع. كما تساهم هذه الحملات في إيقاظ الضمائر وتوعية الأفراد بمخاطر الأمراض الخطيرة، وتعاطي الكحول والتدخين، وحوادث الطرق التي تكلف الدولة مليارات من العملة سنويًا. بالإضافة إلى ذلك، تساهم هذه الحملات في تقليل الحاجة إلى التدخلات التنظيمية المباشرة، مثل إصدار القوانين أو فرض الحلول بالقوة، من خلال تعزيز الوعي الذاتي والمسؤولية الاجتماعية. (عبير، 2012، ص 94)
8. تهدف الحملات الإعلامية إلى إقناع الجماهير المستهدفة بإحداث تعديلات تدريجية في مواقفهم تجاه قضايا سياسية أو اقتصادية أو اجتماعية، من خلال استخدام استراتيجيات وأساليب متوافقة ومقبولة لديهم، تساهم في تعزيز قبول هذه التغييرات وتحقيق الأهداف المرجوة بشكل تدريجي وفعّال.
9. هدف الحملات الإعلامية إلى تحسيس الرأي العام بقضايا مجتمعية محددة لضمان عدم تعرضها للنسيان أو التغاضي، مثل تنظيم حملات توعية لفئة ذوي الإعاقة وذوي الاحتياجات الخاصة، أو ضحايا الكوارث والفئات الاجتماعية المحرومة.

وتعمل هذه الحملات على تنبيه المجتمع وتحفيزه على تعزيز قيم التضامن، والتكافل، والتعاون الاجتماعي، مما يسهم في بناء مجتمع أكثر تماسكًا وتضامنًا.

4.2. خصائص الحملات الإعلامية:

يرتبط مفهوم الحملة الإعلامية ارتباطًا وثيقًا بمفهوم إعادة التشكيل أو الإصلاح، سواء على مستوى الفرد أو على مستوى البناء الاجتماعي، فحيثما وجد مفهوم الحملة، يترافق معه بالضرورة مفهوم إعادة التشكيل، إذ تهدف الحملات عادةً إلى قيادة أفراد المجتمع نحو حالة أفضل ولهذا، يميز بعض الباحثين منهجين رئيسيين كسمات مميزة للحملات الإعلامية، وهما: منهج الضبط الاجتماعي ومنهج العملية.

1- منهج الضبط الاجتماعي:

يرتكز هذا المنهج على ثلاثة محاور رئيسية:

1. **التعليم** :يهدف إلى تقديم كافة المعلومات والعناصر المتعلقة بالمشكلة أو القضية موضوع الحملة، لرفع مستوى وعي الجمهور.
2. **التدبير** :يركز على اتخاذ الإجراءات الإرشادية والتوجيهية التي تساعد الأفراد على التعامل الصحيح مع القضية أو المشكلة المطروحة.
3. **التعزيز أو التدعيم** :يعتمد على إصدار القوانين والتعليمات التي تلزم الجمهور بالتفاعل الإيجابي مع القضية المطروحة.

2- منهج العملية:

يشمل هذا المنهج عمليات تخطيط الرسائل واختيار الوسائل الإعلامية المناسبة، بناءً على خصائص الجمهور المستهدف. كما يتضمن وضع خطط لإدارة الحملة وتقييم نتائجها لضمان تحقيق الأهداف المنشودة.

تتميز الحملات الإعلامية بكونها نشاطًا اتصاليًا مؤسسيًا وجماعيًا، يتوافق مع المعايير والقيم السائدة، ويهدف إلى توجيه ودعم وتحفيز اتجاهات الجمهور نحو أهداف

اجتماعية مقبولة. وهذا التميز يمنح الحملات الإعلامية مصداقية عالية لدى جماهيرها، لارتباطها الوثيق بقضاياهم الاجتماعية وقدرتها على معالجة العديد من الظواهر.

ومن الخصائص الجوهرية للحملات الإعلامية ما يلي:

- **التكرار:**

تعمل الحملة الإعلامية على تحقيق ثلاثة أهداف من خلال عملية تكرار الرسائل:

- تثبيت الرسائل في ذاكرة الجمهور المستهدف بحيث يتم استرجاعها تلقائيًا عند الحاجة.
- دفع الجمهور لتقبل الرسائل عن طريق الإلحاح والتكرار.
- إتاحة الفرصة لفئات أوسع من الجمهور للتعرف على مضمون الرسائل.

- **الاستمرارية:**

تعني عدم التوقف المؤقت أو النهائي عن بث الرسائل ضمن الفترة الزمنية المحددة للحملة، إذ يجب أن تستمر الأنشطة والبرامج دون انقطاع للحفاظ على التواصل الفعّال بين القائمين على الحملة والجمهور المستهدف، ما يعزز فرص تحقيق الأهداف المرجوة.

- **استخدام كافة وسائل الاتصال:**

يُفترض أن تستخدم الحملات الإعلامية جميع وسائل الاتصال المتاحة، بحسب الإمكانيات المادية والبشرية للقائمين عليها، وبما يتناسب مع طبيعة الجمهور المستهدف. هذا الاستخدام الشامل يضمن وصول الرسالة إلى أكبر شريحة ممكنة من الجمهور، ويقلل من احتمال عدم وصولها لأي فئة مستهدفة.

- **كثافة التغطية:**

تعبر عن الجهود المكثفة في إغراق الجمهور المستهدف بسيل من الرسائل التي تحمل آراء وأفكار ومعتقدات القائمين على الحملة. ويمكن تمييز نوعين من الحملات من حيث

كثافة التغطية وفقًا لأهداف الحملة وخصائص الجمهور. (لرقاب، 2020 – 2021، ص77)

- **ذات إدارة منظمة:**

تعني وجود تخطيط محكم ومنهجي للعمل، حيث يتم رسم مسار واضح يقود إلى تحقيق الهدف المرجو. ويستلزم التخطيط جمع المعلومات والبيانات اللازمة لمحتوى نشاط الحملة الإعلامية، مما يجعل الحملة ذات إدارة منظمة وجهود منسقة. هذا التنظيم يُمكّن القائمين على الاتصال من اختيار أنجع الطرق وأقصرها لتحقيق الهدف في زمن مناسب، مع تقليل الجهد والموارد المستهلكة.

- **ذات مدة زمنية محددة:**

تشترط الحملات الإعلامية تحديد فترة زمنية واضحة للبداية والنهاية، بحيث لا تكون طويلة الأمد. فالفترة الزمنية المحددة تُحفّز الحملة على تكثيف الجهود للوصول إلى الأهداف بأسرع وقت ممكن وبأقل تكلفة. هذا التكثيف يمنع شعور الجمهور بالملل الناتج عن التكرار المستمر للرسائل، والذي قد يؤدي إلى إحباط القائمين على الحملة ويعرقل تحقيق الهدف. من جهة أخرى، يجب ألا تكون مدة الحملة قصيرة جدًا بحيث تعيق القائمين على الحملة من إنجاز الأنشطة المطلوبة، كما يجب ألا تتجاوز الحد المعقول لكيلا يشغل ذلك الجمهور عن انشغالاتهم اليومية . (نسيمة، مقبل. 2019 / 2020، ص 12)

ويمكن تلخيص هذه الخصائص فيما يلي:

1-**الاتساع والانتشار:**

تتميز الحملة باستخدام عدة وسائل إعلانية متنوعة تُستهدف بها جميع الفئات والجماهير، مما يضمن وصول الرسائل إلى نطاق واسع من الجمهور.

2-**التركيز على عدد معين:**

تستهدف الحملة مجموعة محددة من الجمهور، مع إمكانية اختلاف الرسائل الإعلانية لتناسب الخصائص والاحتياجات المختلفة لكل فئة.

3-**التوجه الجغرافي:**

تسعى الحملة للوصول إلى الجماهير المنتشرة في مختلف المناطق التي تحتوي على مراكز استهلاك مهمة، لضمان تغطية شاملة وفعالة.

4-**الفترة الزمنية الطويلة:**

تمتد فترة الحملة عادة لمدة سنة أو أكثر، مما يسمح بتحقيق تأثير مستدام وبناء علاقة مستمرة مع الجمهور المستهدف .(إسماعيل، 2018، ص 245.)

5.2. عوامل نجاح الحملات الإعلامية:

لضمان نجاح الحملات الإعلامية، يجب مراعاة مجموعة من العوامل المرتبطة بالرسالة الإعلامية، وهي:

1. **إثارة الانتباه:** يجب أن تجذب الرسالة انتباه الجمهور وتثير اهتمامه بطريقة فعّالة، وذلك باستخدام مؤثرات قوية مثل الكلمات الجذابة، الصور، والرسوم التوضيحية المناسبة في مختلف الوسائل الإعلامية.
2. **وضوح المفهوم:** ينبغي أن يكون مضمون الرسالة بسيطًا وواضحًا ومفهومًا للجمهور المستهدف، باستخدام لغتهم وأساليبهم، لأن الرسالة غير المفهومة لن تحقق التأثير المطلوب.
3. **الرسالة ذات الدلالة:** يجب صياغة الرسالة بدقة بحيث تشرك الجمهور المستهدف وتجعله جزءًا منها، وذلك عبر ما يُعرف بـ«النداء» الذي يحفز الأفراد على تبني الأفكار والسلوكيات المنشودة.
4. **تركيز الفكرة:** يجب أن تحتوي الرسالة على فكرة واحدة أو موضوع واحد فقط، لتجنب تشتيت انتباه المتلقي، مع ضرورة وضوح المصدر الذي يصدر عن الرسالة.
5. **الصفات الشكلية للرسالة:** يجب الانتباه إلى التصميم الجيد للرسالة، سواء في النصوص المكتوبة أو المواد المرئية والمسموعة، بحيث تكون مقروءة وواضحة، مع اختيار مناسب للممثلين، والموسيقى، والأصوات المصاحبة.

6. **الاختبار القبلي:** من الضروري اختبار مجموعة من الرسائل على عينة من الجمهور المستهدف قبل إطلاق الحملة، لتقييم فعاليتها وإجراء التعديلات اللازمة لتجنب هدر الوقت والجهد.
7. **الاحتكار الإعلامي:** من الأفضل أن تُعرض الرسالة على جميع وسائل الإعلام في وقت محدد، مع تنسيق الرسائل بين مختلف وسائل الاتصال لضمان توحيد السياق وعدم التضارب.
8. **التكامل بين وسائل الاتصال:** يجب دمج وسائل الاتصال الشخصية مع وسائل الإعلام الجماهيري، حيث أن التفاعل والمناقشة بين الأفراد تدعم الرسالة وتعزز فرص نجاح الحملة.
9. **تكثيف الحوافز:** من المهم توفير وتحفيز الحوافز لدى الجمهور، لتعزيز مشاركتهم وتحقيق أهداف الحملة بفعالية. (يوسف، 2018 ، ص 44 . 45 .)

6.2. مراحل إعداد حملة إعلامية.

أولاً ـ التعرف على المشكلة:

تعني هذه المرحلة جمع المعلومات والإحصائيات والبيانات الكافية المتعلقة بالمشكلة موضوع الدراسة أو البحث، وفهم أبعادها الحقيقية. ترتبط صياغة المشكلة ارتباطًا وثيقًا بأهداف الحملة وطبيعة الظاهرة الاجتماعية التي تستهدفها، حيث يتم تحديد مختلف الأبعاد المرتبطة بالظاهرة الاجتماعية السلبية التي تسعى الحملة إلى تغييرها أو القضاء عليها.

ولتحديد المشكلة بدقة، يُطرح مجموعة من الأسئلة الأساسية، منها:

- ما هو الهدف الرئيسي من الحملة؟
- ما السلوك المحدد الذي نرغب في تغييره لدى الجمهور المستهدف؟
- ما هي المعتقدات الاجتماعية الخاطئة التي تستهدف الحملة تعديلها أو إلغائها؟
- ما هو السلوك المرجو تحقيقه بعد تنفيذ الحملة؟ (زعموم، ص 32)

ثانيًا ـ تحديد وصياغة أهداف الحملة:

يقصد بالهدف الصورة الذهنية للحالة المستقبلية أو الغايات التي تُوضع من أجلها خطة الحملة، حيث تُعد الأهداف العنصر الرئيسي والأساسي الذي تعتمد عليه أي خطة ناجحة.

من الضروري صياغة الأهداف بدقة بحيث تكون قابلة للقياس والمتابعة في المستقبل، ويجب أن تركز هذه الأهداف على معالجة المشكلة الأساسية التي استُهدفت بها الحملة. فلا يمكن لأي حملة تحقيق نجاح فعلي دون تحديد أهداف واضحة ومحددة من البداية.

السعي بدون معرفة الأهداف الأساسية يؤدي غالبًا إلى نتائج ضعيفة أو فاشلة، لذا يُعتبر تحديد الأهداف من أهم أساسيات نجاح حملات التوعية الإعلامية. تختلف أهداف هذه الحملات حسب الحاجة، فقد تهدف بعضها إلى رفع الوعي العام لدى فئة معينة حول قضية معينة دون السعي لتغيير الاتجاهات أو السلوكيات. في حين تهدف حملات أخرى إلى تحقيق التغيير المعرفي، أو التغيير في الاتجاهات، أو التغيير السلوكي، وقد تجمع الحملة بين هذه الأهداف جميعًا، وهو ما يعد الهدف الأمثل الذي تسعى إليه معظم الحملات الناجحة. (صالح محمد الملك، هـ1421)

ثالثًا ـ تحديد الجمهور المستهدف في الحملة الإعلامية:

يُعدّ الجمهور المستهدف العنصر الرئيسي والمحوري في العملية الاتصالية، وهو الهدف الأساس الذي يسعى القائمون على الحملات الإعلامية إلى الوصول إليه والتأثير فيه. فنجاح الحملة الإعلامية يعتمد بدرجة كبيرة على مدى دقة تحديد هذا الجمهور، وفهم خصائصه، واحتياجاته، وسلوكياته.

ينطلق مبدأ أساسي في الاتصال الفعال يتمثل في" :**اعرف جمهورك**"، وهو ما يتطلب إجراء دراسات مسبقة لفهم الفئة المستهدفة من حيث العمر، والجنس، والمستوى التعليمي، والموقع الجغرافي، والثقافة، والميول، والمواقف، وطرق تلقيهم للمعلومة.

فإذا لم تتمكن الحملة من الوصول إلى جمهورها الحقيقي، فلن تستطيع التأثير فيه أو دفعه نحو التغيير المطلوب. لذلك، فإن تحديد الجمهور بدقة ليس مجرد خطوة إجرائية، بل هو قاعدة أساسية تُبنى عليها باقي مراحل التخطيط للحملة الإعلامية، مثل اختيار الرسائل المناسبة، والوسائل الفعالة، وتوقيت التنفيذ. (زكرياء، 2013، ص 1. 6 .)

يُعدّ الجمهور المستهدف العنصر المحوري في العملية الاتصالية، وهو الهدف الأساسي الذي تُبنى عليه كل استراتيجيات الحملات الإعلامية. فنجاح أي حملة يعتمد بدرجة كبيرة على مدى دقة تحديد هذا الجمهور، وفهم خصائصه وسلوكياته وطرق تفاعله مع الرسائل الإعلامية.

ينطلق مبدأ جوهري في الاتصال الفعال يتمثل في" :**اعرف جمهورك**"، وهو ما يتطلب دراسة معمّقة لخصوصيات هذا الجمهور، وفهم احتياجاته، ورغباته، وعاداته، وأنماط تعرضه لوسائل الإعلام المختلفة. ويتم ذلك من خلال خطوتين أساسيتين:

1. دراسة الجمهور:

تُعنى هذه الخطوة بجمع معلومات شاملة عن الفئات الاجتماعية التي تمسّها الحملة، وتشمل:

- احتياجاتهم ورغباتهم.
- آراؤهم واتجاهاتهم.
- مستوياتهم التعليمية والثقافية.
- عاداتهم وسلوكياتهم.
- خصائصهم السوسيوديموغرافية (السن، الجنس، المهنة) .
- تركيبتهم السيكولوجية والاجتماعية.

2. تصنيف الجمهور:

تتمثل هذه الخطوة في تجزئة الجمهور إلى فئات متجانسة تُسهل عملية الاستهداف، وذلك على النحو التالي:

- **الجمهور الأولي** :هو الجمهور الرئيسي الذي تسعى الحملة الإعلامية إلى التأثير فيه بشكل مباشر.
- **الجمهور الثانوي:** هو الجمهور الداعم، الذي يمكن أن يسهم في نجاح الحملة بصورة مباشرة أو غير مباشرة، من خلال تأثيره على الجمهور الأولي أو دعمه لمحتوى الحملة.

إن تحديد الجمهور المستهدف بدقة لا يُعد مجرد خطوة تقنية، بل هو قاعدة تُبنى عليها كل مكونات الحملة، من الرسالة الإعلامية إلى اختيار الوسائل والأنشطة والتوقيت، وبالتالي فإن إغفال هذه المرحلة أو تنفيذها بشكل سطحي يُعرض الحملة للفشل أو ضعف الأثر. (الكافي، 2015 ، ص193)

رابعًا ـ تحديد رسائل الحملة:

تُعد الرسالة الإعلامية جوهر الحملة ومفتاح نجاحها، إذ إنها الوسيلة الأساسية التي يتم من خلالها نقل الأفكار والمضامين إلى الجمهور المستهدف. ويُعزى فشل أو نجاح أي حملة إعلامية بدرجة كبيرة إلى فعالية الرسائل المصممة ومدى توافقها مع طبيعة الجمهور.

ولا يمكن صياغة رسائل ناجحة ومؤثرة دون فهم عميق للجمهور المستهدف؛ فلكل فئة اجتماعية أو عمرية أو ثقافية طريقة خاصة في استقبال الرسائل وفهمها والتفاعل معها. لذلك، ينبغي أن تراعي الرسائل الخصائص النفسية والاجتماعية والمعرفية للجمهور. فمثلًا:

- الرسائل الموجهة للأطفال أو صغار السن يجب أن تكون مبسطة، جذابة، ومرئية قدر الإمكان.
- الرسائل الموجهة للمثقفين ينبغي أن تحتوي على مضمون عقلاني مدعوم بالحجج المنطقية والمعطيات.
- أما الرسائل الموجهة إلى فئات النفوذ أو التأثير، مثل المسؤولين أو العلماء أو رجال الفكر، فيجب أن تكون مؤسسة ومبنية على أدلة وأبعاد استراتيجية.

- كما يمكن توظيف الشخصيات العامة كالفنانين أو الرياضيين أو المؤثرين الاجتماعيين لإضفاء مصداقية وانتشار أكبر للرسائل، باعتبارهم يتمتعون بجاذبية وتأثير في أوساط جماهيرية واسعة.

وتتطلب الرسالة الفعالة في إطار الحملة الإعلامية أن تتسم بعدة صفات، من بينها:

- الوضوح والسهولة في اللغة والمضمون.
- التركيز على فكرة واحدة لتجنب تشتيت الانتباه.
- الارتباط المباشر بهدف الحملة.
- القدرة على إثارة الانتباه والانفعال الإيجابي.

إن بناء الرسالة يتطلب عناية فائقة، لأنها الأداة التي ستقود في النهاية إلى تغيير معرفي أو اتجاهي أو سلوكي لدى الجمهور المستهدف، وهو ما تسعى الحملة إلى تحقيقه.

خامسًا ـ اختيار وانتقاء الوسيلة الإعلامية:

يُعد اختيار الوسيلة الإعلامية أحد أهم القرارات الاستراتيجية في الحملات الإعلامية، فهو لا يُبنى بشكل اعتباطي، بل يرتكز على مجموعة من العوامل الأساسية، أبرزها :طبيعة الرسالة، خصائص الجمهور المستهدف، ونوعية المشكلة المطروحة .فالوسيلة يجب أن تتناسب مع المحتوى المراد توصيله، ومع الوسيط الأفضل لنقله إلى الفئة المعنية بفعالية وتأثير.

وتتعدد الوسائل التي يمكن استخدامها حسب طبيعة الحملة، مثل:

- الصحافة المتخصصة لنقل الرسائل التحليلية أو الموجهة إلى فئات مثقفة.
- الإذاعة والتلفزيون لبلوغ شريحة واسعة من المجتمع بسرعة.
- السينما أو الوثائقيات لتقديم محتوى عاطفي عميق يؤثر على الرأي العام.
- الملصقات والمنشورات في الحملات الميدانية أو التوعوية المحددة.
- وسائل التواصل الاجتماعي اليوم تلعب دورًا متزايدًا في الحملات الإلكترونية والتفاعلية.

إن اختيار الوسيلة يجب أن يكون مدروسًا جيدًا، ويُحدد أيضًا بناءً على تقسيم الميزانية المخصصة للحملة بين الوسائل المختلفة، مع الأخذ بعين الاعتبار الوصول، الفعالية، والتكلفة.

سادسًا ـ تحديد الموارد المتاحة:

لا يمكن تنفيذ حملة إعلامية ناجحة دون ضبط دقيق للموارد المتاحة، سواء كانت مالية، بشرية أو لوجستية. فبعد وضع الخطة الاتصالية الكاملة، من الضروري إجراء تقييم شامل للموارد المطلوبة وتقدير الميزانية الضرورية لتنفيذ الأنشطة المقترحة.

ويُعد تحديد الموارد مرحلة مفصلية، لأنه:

- يسمح بتنظيم الجهود البشرية وتحديد الكفاءات المطلوبة.
- يساهم في تقدير التكاليف الفعلية للحملة على مراحلها المختلفة.
- يضمن الاستغلال الأمثل للإمكانات المتوفرة ويقلص من الهدر.

كما يمكن تصنيف الموارد إلى:

- موارد حالية ومضمونة متوفرة لدى الجهة القائمة بالحملة.
- موارد محتملة يمكن الحصول عليها من خلال شراكات، رعاة، أو دعم حكومي أو مؤسساتي.

سابعًا ـ تحديد المخطط الإداري والتنظيمي:

تعتمد الحملة الإعلامية الناجحة على هيكلة إدارية وتنظيمية واضحة، تُسند من خلالها المهام وتُحدد المسؤوليات، مما يضمن تنسيق الجهود وتفادي التداخل أو الفوضى. في هذه المرحلة، يتم:

- توزيع الأدوار على فرق العمل المختلفة (إعداد الرسائل، النشر، التقييم...).
- وضع هيكل تنظيمي إداري مرن يسمح بالمتابعة اليومية.
- تحديد العراقيل القانونية والتنظيمية المحتملة، ووضع خطط لتجاوزها.

ويختلف أسلوب التنظيم من حملة لأخرى حسب طبيعة النشاط وأهداف الحملة، ويمكن اعتماد ثلاث طرق رئيسية في إدارة الحملة:

1. **الطريقة الأولى – الإدارة المتكاملة:** تعتمد على تشكيل إدارة مستقلة داخل الهيكل التنظيمي للمؤسسة، تضم مختصين وتقود أنشطة الحملة بشكل دائم ومنظم.
2. **الطريقة الثانية – الاستعانة بمستشار خارجي:** يُمكن أن يكون فردًا متخصصًا أو وكالة اتصال تتكفل بتخطيط وتنفيذ وتقييم الحملة.
3. **الطريقة الثالثة – الدمج بين الطريقتين:** حيث يجري التنسيق بين الإدارة الداخلية للمؤسسة وخبرات خارجية لضمان فعالية أكبر. (الكافي، 2015 ، ص98)

ثامنا ـ وضع جدول زمني للحملة الإعلامية: اختيار الوقت المناسب لتنفيذ الحملة الإعلامية. (وآخرون د.، جوان 2017 ص 45)

ثامنًا ـ تقييم الحملة الإعلامية:

يُعد التقييم خطوة محورية في دورة الحملات الإعلامية، فهو الأداة التي تسمح بالتعرف على مدى فعالية الجهود المبذولة، وتحديد مدى تحقيق الأهداف المرسومة. وينقسم التقييم إلى مرحلتين أساسيتين:

1. التقييم القبلي (قبل التنفيذ الفعلي):

يتم في هذه المرحلة اختبار نسخة مصغرة أو أولية من الحملة على عينة ممثلة من الجمهور المستهدف. والهدف من هذا التقييم القبلي هو:

- قياس ردود الفعل المبدئية تجاه الرسالة والوسيلة المستخدمة.
- تحليل مدى وضوح الرسالة وتأثيرها وإمكانية فهمها.
- مدى ملاءمة الوسيلة المختارة لطبيعة الجمهور والسياق.
- تقدير الفعالية المحتملة للحملة من خلال اختبار تفاعلي محدود.

كما يُراعى في هذا النوع من التقييم دراسة جميع عناصر الحملة: اللغة، الأسلوب، التوقيت، الوسائل، وحتى القائمين بالاتصال، لتحديد مدى قدرتها على تحقيق الأهداف المسطرة قبل الشروع في التنفيذ الشامل.

2. التقييم البَعدي (بعد التنفيذ النهائي):

بعد الانتهاء من تنفيذ الحملة بكامل مكوناتها، يأتي دور التقييم النهائي الذي يهدف إلى:

- تحديد نقاط القوة والضعف في تخطيط وتنفيذ الحملة.
- قياس النتائج المحققة مقارنة بالأهداف المسطرة (رفع الوعي، تغيير السلوك، التأثير المعرفي) .
- تحليل العوائق التي واجهت الحملة والطرق التي تم تجاوزها بها أو لم تُعالج.
- تقديم توصيات واضحة للاستفادة من التجربة وتطوير الحملات المستقبلية.

كما يمكن اعتماد أدوات قياس كمية (كالاستبيانات والتحليل الإحصائي للنتائج) وأخرى نوعية (كالمقابلات والملاحظات المباشرة وتحليل المحتوى) لضمان شمولية التقييم وصدقة. (قراي، ص 53)

الفصل الثالث:

أشكال الانتهاكات وآليات حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي

3. أشكال الانتهاكات وآليات حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي.

تمهيد:

شهد العالم خلال العقود الأخيرة ثورة رقمية هائلة، كان من أبرز ملامحها انتشار شبكات التواصل الاجتماعي التي أصبحت جزءًا لا يتجزأ من الحياة اليومية للأفراد، ووسيلة رئيسية للتفاعل وتبادل المعلومات. إلا أن هذا التطور التقني المتسارع ترافق مع تحديات قانونية وأمنية جديدة، أبرزها ما يتعلق بخصوصية المستخدمين وحماية بياناتهم الشخصية. فقد أصبحت هذه الشبكات بيئة خصبة لمختلف أشكال الانتهاكات، كالتجسس، وسرقة البيانات، والتنمر الإلكتروني، وغيرها من الممارسات التي تهدد خصوصية الأفراد وسلامتهم الرقمية.

وفي ظل هذه التهديدات المتزايدة، برزت الحاجة إلى وضع آليات فعالة لحماية الخصوصية الرقمية، سواء من خلال الأطر القانونية والتنظيمية، أو عبر تطوير وسائل تقنية وأمنية متقدمة تضمن الاستخدام الآمن والمسؤول لهذه المنصات. ومن هنا تأتي أهمية دراسة أشكال الانتهاكات التي تطال مستخدمي شبكات التواصل الاجتماعي، وتحليل سبل التصدي لها، بهدف المساهمة في تعزيز ثقافة الوعي الرقمي وبناء فضاء إلكتروني أكثر أمانًا.

1.3. مفهوم حماية الخصوصية

1- مفهوم حماية الخصوصية:

يرجع أصل كلمة الخصوصية في اللغة العربية إلى الفعل خص، فيقال: خص فلانا بالشيء، بمعنى فضله به وأفرده، ويقال كذلك خصه بالود، أي حبه دون غيره، وخاصة الشيء ما يختص به دون غيره، أي ينفرد به، والخصوص يقابله العموم، كما يفيد الحصر وشدة الإطلاق، والخاصة ما تخصه لنفسك، ويقال فلان يخص فلان، أي خاص به، والخصوصية بالفتح أفصح، ومنه قول الله تعالى في سورة البقرة: "الله يختص برحمته من يشاء والله ذو الفضل العظيم"، أما في اللغة الانجليزية فتعني لفظة الخصوصية (privacy) حالة العزلة و الانسحاب من صحبة الآخرين، كما تستخدم لتدل على الطمأنينة و السلم و الوحدة و الانسحاب من الحياة العامة للأفراد.

يُعد تحديد مفهوم الخصوصية في مواقع التواصل الاجتماعي من أبرز القضايا القانونية التي أولتها التشريعات المعاصرة اهتمامًا بالغًا، وذلك بهدف تمكين مستخدمي هذه المنصات من الحفاظ على خصوصيتهم الشخصية. وتُعرَّف الخصوصية بأنها حق الفرد في التحكم بالمعلومات الخاصة به، وتحديد متى وكيف وإلى أي مدى يمكن للآخرين – سواء المستخدمين أو القائمين على المنصة – الوصول إلى تلك المعلومات. ومن هذا المنطلق، يتبين أن لكل شخص الحق في الحماية من أي تدخل غير مبرر في شؤونه الشخصية، بالإضافة إلى حقه في اختيار الوسيلة المناسبة التي يعبّر من خلالها عن أفكاره ورغباته وسلوكياته، وذلك في إطار ما تتيحه تقنيات هذه المنصات من أدوات وإمكانات للتواصل والتعبير. (سيد، 2013 ص13)

وعلى هذا الأساس، تُفهم الخصوصية في مواقع التواصل الاجتماعي، في أبسط صورها، على أنها تتعلق بسرية الحياة الشخصية لمستخدمي هذه المنصات. وتشمل تلك الخصوصية جميع الوقائع والمعلومات المخزنة سواء على أجهزة الحاسب الآلي الشخصية أو الهواتف الذكية، أو تلك التي تم حفظها على حسابات المستخدمين ضمن مواقع التواصل

الاجتماعي. وتكمن الخطورة في إمكانية تعرّض هذه البيانات للاختراق أو السرقة، حيث يُعد أي اعتداء عليها أو كشفها دون إذن من المستخدم انتهاكًا واضحًا للخصوصية. ويشمل ذلك أيضًا أعمال التجسس الإلكتروني، أو اعتراض الرسائل البريدية المرسلة بقصد الاطلاع عليها أو معرفة محتواها، وما قد يترتب على ذلك من إفشاء لأسرار ذات طابع اقتصادي أو سياسي أو اجتماعي أو صحي أو علمي، مما يُعد من أخطر أشكال الانتهاكات التي تهدد الأمن المعلوماتي والخصوصي للمستخدمين.

تُعد حماية الخصوصية في مواقع التواصل الاجتماعي من أبرز الحقوق المرتبطة بحرية الفرد في إدارة معلوماته الشخصية، حيث يتمثل جوهر هذا الحق في قدرة الشخص على التحكم في بياناته وتحديد ما يُكشف منها ولمن. وقد أولت التشريعات الحديثة هذا المفهوم اهتمامًا خاصًا، إدراكًا منها لأهمية حماية الخصوصية المعلوماتية لمستخدمي الإنترنت. وبناءً عليه، يمكن تعريف حماية الخصوصية المعلوماتية بأنها حماية البيانات الشخصية الخاصة بمستخدمي مواقع التواصل عند تعاملهم عبر الشبكة.

وبالاستناد إلى ما سبق، يتضح أن المستخدم يُعد العنصر الأساسي والمحرك الفعلي لشبكات التواصل الاجتماعي، والتي لا يمكن استخدامها إلا من خلال الإنترنت. وقد عرّفه الفقه بأنه "الشخص الذي ينضم إلى الشبكة ويتنقل في فضاء الإنترنت للحصول على المعلومات أو نشرها"، وبذلك يجمع المستخدم بين كونه مستهلكًا حين يتلقى المحتوى، ومورِدًا عندما يعبّر عن آرائه أو ينشر أعماله عبر صفحته الخاصة، فيتحول إلى مؤلف وناشر في آن واحد. أما مقدم خدمة التواصل، فيُنظر إليه كمستضيف للصفحة فقط، إذ يقتصر دوره على تخزين المحتوى وإتاحته للجمهور أو من يحدده المستخدم، دون التدخل في المضمون. ويُشترط في من يرغب باستخدام شبكات التواصل أن يكون شخصًا طبيعيًا يبلغ سنًا معينة تحددها كل منصة على حدة، وألا يكون قد أُدين في جرائم تمس الشرف أو الأخلاق ما لم يُرد إليه اعتباره. كما يتوجب عليه عند التسجيل الإقرار بقراءته لسياسة استخدام البيانات

الشخصية وموافقته عليها، بعد تعبئة البيانات الإلزامية التي يطلبها مقدم الخدمة، وتُستخدم لاحقًا لأغراض تجارية.

وتتضمن البيانات الإلزامية الاسم، العمر، الجنس، والبريد الإلكتروني ورقم الهاتف، الحالة الاجتماعية والجنسية والمعتقدات الدينية، مع إمكانية إضافة بيانات مهنية واختصاصية لاحقًا. وهذه المعلومات تُعد بيانات شخصية ترتبط بشخص معين، إلا أنه من الناحية العملية لا يوجد ما يمنع المستخدم من إدخال معلومات غير دقيقة، كعمر أو تاريخ ميلاد وهمي.

وخلاصة القول، إن أساس حماية البيانات الشخصية هو أن تكون هذه البيانات مرتبطة بشخص محدد أو يمكن تحديده استنادًا إلى ما تم إدخاله من معلومات، أما إن كانت البيانات لا تعود إلى شخص معروف أو يمكن التعرف عليه، فلا محل للقول بوجود حماية لها لغياب الخصوصية.

ومن جهة أخرى، تحرص شبكات التواصل الاجتماعي على تضمين شروط العضوية ما يمنحها الحق في إزالة الحسابات التي تتضمن بيانات زائفة أو محتوى مخالف للقانون، وذلك فور تلقي شكاوى موثقة أو اكتشاف المخالفة أثناء المعالجة. مع ذلك، يُمنح المستخدم الحق في الطعن على قرارات الإزالة، خاصة إذا ثبت أن تلك الإجراءات استندت إلى تحليل غير دقيق من جهة مقدم الخدمة. (الصادق، 2016، ص77)

2- سياسة الخصوصية لدى مواقع التوصل الاجتماعي:

أدركت مواقع التواصل الاجتماعي أهمية حماية خصوصية المستخدمين، مما دفعها إلى اعتماد آليات محددة، أبرزها وضع سياسات الخصوصية، بهدف توفير هذه الحماية. وتُعرف سياسة الخصوصية بأنها بيان قانوني يوضح كيفية جمع ومعالجة بيانات المستخدمين والزوار من قبل الشركة أو الموقع، كما يحدد الآليات التي سيتم عبرها التعامل مع المعلومات التي تم جمعها، سواء من خلال مشاركتها مع أطراف أخرى أو الحفاظ على سريتها. ومن هذا المنطلق، يقع على عاتق مواقع التواصل الاجتماعي التزامٌ بنشر سياسات

الخصوصية الخاصة بها على منصاتها الرسمية، وذلك لعدة أسباب رئيسية، من أبرزها ضمان الشفافية تجاه المستخدمين وحماية بياناتهم الشخصية وفقًا للمعايير القانونية والأخلاقية.

- يعد إظهار سياسة الخصوصية التزامًا قانونيًا تفرضه التشريعات المعاصرة، إذ يتوجب على مواقع التواصل الاجتماعي نشر هذه السياسة بشكل واضح، وذلك لتحميلها مسؤولية قانونية مباشرة تجاه كيفية جمع البيانات واستخدامها، وضمان حماية حقوق المستخدمين في خصوصية معلوماتهم الشخصية.
- تُعتبر سياسة الخصوصية متطلبًا من قِبل الأطراف الثالثة، إذ تلزم شركات كبرى مثل Google وAmazon، المواقع الإلكترونية والتطبيقات التي تستخدم خدماتها بضرورة نشر سياسة خصوصية واضحة. وتشترط هذه الشركات أيضًا الحصول على إذن صريح من المستخدمين قبل جمع أو مشاركة بياناتهم الشخصية، نظرًا لأن الإعلانات المدمجة ضمن المواقع أو التطبيقات تقوم بجمع معلومات المستخدمين، مما يستدعي ضمان حماية خصوصيتهم والامتثال للمعايير القانونية والتنظيمية.
- يُستخدم إعداد سياسة الخصوصية كوسيلة لزيادة الشفافية، حيث ترى الشركات الكبرى ومواقع التواصل الاجتماعي أن بناء الثقة مع العملاء والمستخدمين يمثل عنصرًا أساسيًا في علاقتها بهم. ولهذا الغرض، تقوم هذه الجهات بوضع سياسات خصوصية واضحة ومفهومة، تُمكن المستخدمين من معرفة مصير المعلومات التي يتم جمعها عنهم، مما يسهم في تعزيز الثقة المطلوبة. فسياسة الخصوصية تمنح المستخدمين إحساسًا بالأمان من خلال تمكينهم من التحكم ببياناتهم الشخصية وفقًا لما تحدده تلك السياسة، التي ينبغي أن تشرح للمستخدمين بوضوح كيفية التعامل مع بياناتهم، والأسباب التي تستدعي جمعها، والفترة الزمنية التي سيتم خلالها الاحتفاظ بهذه البيانات. وتتضمن سياسة الخصوصية توضيح مجموعة من النقاط التالية:

- المعلومات التي تجمع وكيفية استخدامها، وقد تكون هذه المعلومات قد صرح بها المستخدم، أو معلومات يتم جمعها أليا.
- كيفية حفظ وحماية هذه المعلومات.
- معلومات عن كيفية التواصل مع الشركة أو الموقع.
- إعلام المستخدمين بالوسائل المستخدمة لجمع معلوماتهم وتتبع سلوكياتهم مثل استخدام ملفات تعريف الارتباط (Cookiet) وملفات الدخول والتتبع.
- إعلام المستخدمين بسياسة الخصوصية حيث يجب إعلام المستخدمين عن حقهم في إلغاء الانتساب والاشتراك في المواقع او في جوانب وخدمات معينة يقدمها الموقع. (Maria Pirzada, sample privacy policy template, https://www.privacypolicies.com/blog/privacy-policy-template, consulté le 25/08/22، 18:55)

2.3. أشكال انتهاكات الخصوصية لدى مستخدمي شبكات التواصل الاجتماعي

يُشكل الوصول غير المصرح به إلى المعلومات ذات الطابع الشخصي أحد أخطر أشكال انتهاك الخصوصية، وغالبًا ما يكون ناتجًا عن اختراقات أمنية. وتبرز هذه الإشكالية بشكل خاص في مواقع التواصل الاجتماعي، حيث تتيح بعض المنصات، بموجب موافقة المستخدمين على شروط الاستخدام، لنفسها حق التعامل مع بياناتهم الشخصية. وبموجب ذلك، قد تتم مشاركة هذه البيانات مع جهات خارجية مثل الباحثين الأكاديميين، وشركات التسويق والإعلان، وأحيانًا مع الأجهزة الأمنية، في إطار تحقيق مصالح تجارية مباشرة أو غير مباشرة.

يُعد الكشف عن المعلومات الخاصة بالأفراد أو الإعلان عنها دون موافقتهم الصريحة انتهاكًا صارخًا للخصوصية، لا سيما إذا تم ذلك عبر الوسائط الرقمية الحديثة ووسائل الإعلام الإلكترونية. ويتمثل هذا الاعتداء في نشر معلومات حساسة تتعلق بالحالة الصحية،

أو الوضع الاجتماعي، أو التاريخ العلاجي أو النفسي للفرد، دون الحصول على موافقة مسبقة منه، أو خارج الأطر القانونية التي تحمي خصوصيته.

وتتضاعف خطورة هذه الأفعال عند إظهار الشخص المعني بصورة واضحة، سواء من خلال اسمه أو صورته الشخصية، مما يُسهل التعرف عليه واستغلال تلك المعلومات ضده. فإن مثل هذا الاعتداء يُعد خرقًا للحق في الخصوصية، ويُشكل مخالفة قانونية جسيمة تقع ضمن انتهاكات الحقوق الفردية. (امين، 2007، ص 58– 59)

ضمن هذا السياق، أصبحت مواقع التواصل الاجتماعي هدافًا رئيسيا للانتهاكات المتعلقة بالخصوصية، حيث تمكن بعض الأفراد ذوي الكفاءة التقنية من اختراق أنظمتها والوصول إلى معلومات حساسة تخص أعدادًا كبيرة من المستخدمين، مما يشكل تهديدًا واضحًا لأمنهم المعلوماتي وحقهم في حماية خصوصيتهم.

ولقد كشفت الدراسات الأخيرة أن ما نسبته 80 % من الناس يشعرون بالقلق إزاء من يستطيع الوصول إلى بياناتهم على مواقع التواصل الاجتماعي، وقد وقع ما يقرب من ربع مستخدمي هذه المواقع، ضحايا للهجمات على الانترنيت؛ حيث أدى اختراق تويتر في جويلية 2020، إلى زيادة التشكيك في فعالية التدابير التي وضعها مقدموا الخدمات لحماية الخصوصية لمستخدميها.

وفي مارس 2018، كشفت سلسلة من التقارير من الجرائد الكبرى، مثل "نيويورك تايمز"، و"الغارديان"، حقيقة أن كامبريدج التحليلية الرقمية، حصلت على أكثر من 50 مليون، من البيانات الشخصية لمستخدمي فايسبوك، دون موافقتهم، وقد أدى تسرب هذه البيانات، في توليد نوبات نفسية للمستخدمين في الولايات المتحدة الأمريكية، التي عززت حملة "دونالد ترامب" المادية إلى الانتخابات الرئاسية لعام 2016.

ولم يكن فايسبوك منصة التواصل الاجتماعي الوحيدة، التي يعاني مشتركيها من انتهاكات بياناتهم عليها، بل حصل ذلك مع " LinkedIn " أيضا، في عام 2012؛ حيث فقدت الشركة 167 مليون وثيقة اعتماد حساب، بما في ذلك كلمات السر المشفرة، و في عام

2016؛ حيث فقدت شركة " LinkedIn "علنا، بان البيانات التي سرقت، خلال ذلك الهجوم، و كانت تباع على شبكة الانترنيت المظلم.

واستخدمت لينكدإن 20 مليون مستخدم لإجراء تجربة دون موافقتهم أو علمهم. كان لدى الشركة حدس بأن الناس يحصلون على وظائف أكثر من خلال المعارف البعيدة مقارنةً بالعلاقات الشخصية الوثيقة.

لاختبار النظرية، قام موقع LinkedIn بتعديل أنواع الاتصالات التي يعرضها على الأشخاص، مما قد يؤثر على فرص العمل لآلاف المستخدمين.

كما حدث نفس الأمر مع شركة" Twitter "، حيث تمت سرقة 32 مليون كلمة سر عام 2016، وبعد أن اعترفت الشركة، أن أكثر من 330 مليون بطاقة اعتماد تم كشفها في نص بسيط، في عام 2018، وتم استهدافهم بهجوم هندسي اجتماعي عام 2020، ولم يكن عام 2022 استثناءًا بعد استغلال ثغرة أمنية جديدة على الموقع، نشر المتسللون معلومات خاصة لأكثر من 5 ملايين مستخدم للحسابات على سوق الويب المظلم. (https://www.terranovasecurity.com/blog/data-privacy-social-media-protect-your-information، 2025/04/30, 18: 45)

ويمكن تقسيم الأشخاص الذين يقومون بعملية الاختراق إلى ثلاث فئات وهي:

- **الفئة الأولى الفضوليون (المخترقون hackers):** وهم الذين يقومون بالاستمتاع بتنفيذ المهمات الصعبة بل المستحيلة واقتحام اعقد الأنظمة على سبيل الهواية، بهدف إثبات الذات أو النوايا الإجرامية كتدمير البيانات أو الابتزاز.
- **الفئة الثانية المتلصصون (crackers):** وهم الفئة التي تحاول الدخول إلى أنظمة الحاسوب الآلي بسوء نية وبشكل غير قانوني بغرض التخريب، وذلك بتغيير المعلومات أو حذفها أو إضافة معلومات تخدم هدفا معينا.
- **الفئة الثالثة العابثون (vandals):** وهم الفئة التي تخترق بدافع العبث، وينقسمون إلى مجموعتين هما: مجموعة تشكل بعض المستخدمين الذين لهم حق الدخول في

النظام، والمجموعة الثانية من الغرباء الذين لهم حق استخدام النظام أو الدخول فيه، وفي كلتا الحالتين يدخل العابثون بهدف العبث واللهو ويعتقدون أن ما يقومون به من أعمال غير معاقب عليها وهي مباحة. (ابراهيم، 2015)

1. دور المستخدم (المضرور) في انتهاك خصوصيته:

يُعتبر المستخدم نفسه في كثير من الأحيان طرفًا أساسيًا في انتهاك خصوصيته عبر مواقع التواصل الاجتماعي، إذ يقوم بإرادته بكشف معلوماته الشخصية، خصوصًا عند استخدامه خيار "الملف العام"، مما يجعل بياناته متاحة لأي عضو في الموقع. وقد نبّهت بعض المنصات، مثل "فيسبوك"، مستخدميها إلى أن نشر المحتويات باستخدام إعدادات "العام" يتيح للجميع، بمن فيهم غير المستخدمين، الوصول إلى المعلومات واستخدامها (سيد، 2013، ص 89) بناءً عليه، أصبح من الضروري أن تتضمن سياسات الخصوصية في مواقع التواصل الاجتماعي إرشادات واضحة للمستخدمين حول كيفية التعامل مع المعلومات الشخصية التي ينشرها الآخرون عن أنفسهم.

ويمتلك المستخدم الحق في الاعتراض على معالجة بياناته الشخصية لأسباب مشروعة، بما في ذلك رفض استخدامها في الدراسات والأبحاث التجارية، دون أن يُطلب منه تقديم تبريرات، سواء خلال مرحلة جمع البيانات أو في مرحلة لاحقة، (الحكيم، 2007 ، ص 30) كما يحق له رفض الإجابة على الأسئلة المتعلقة ببياناته الشخصية إذا لم يكن هناك التزام بالإفصاح عنها، ورفض إعطاء الموافقة الخطية المطلوبة لمعالجة البيانات الحساسة كالدين أو الجنسية أو الهوايات. كذلك، يجوز للمستخدم المطالبة بحذف بياناته من الملفات التجارية، وذلك من خلال إرسال طلب صريح إلى المسؤول عن المعالجة، الذي يجب أن يرد خلال مهلة محددة قانونًا، مع إلزامه بتقديم مبررات قانونية حال رفضه الطلب.

كما يحق للمستخدم تصحيح أو استكمال أو حذف بياناته متى كانت غير دقيقة أو قديمة أو غير مناسبة أو تمت معالجتها بالمخالفة للقانون. ولا يجوز لأي جهة معالجة البيانات

الشخصية على مواقع التواصل الاجتماعي دون الحصول على إذن صريح من المستخدم، أو دون وجود مبرر قانوني يبرر ذلك، بما لا يمس بحقوقه الأساسية.

على الرغم من أن القوانين المعمول بها تنظم حماية الخصوصية من خلال اشتراط الموافقة، إلا أن الواقع يختلف، إذ غالبًا ما تكون الموافقة على الشروط والأحكام غير واعية، نظراً لطول نصوص السياسات وغموضها. ففي كثير من الأحيان، تُعتبر مجرد ضغطة على زر "أنا موافق" كافية لإنشاء التزام قانوني (عقد إذعان) دون أن تتاح للمستخدم فرصة حقيقية لفهم بنود وشروط الاستخدام.

تتفاقم هذه الإشكالية مع استخدام الأجهزة الذكية التي تفرض على المستخدم الموافقة على مشاركة بياناته بطرق غير واضحة، مثل تبادل البيانات بين تطبيقين مختلفين أو سحب قوائم الأصدقاء وعناوينهم، مما يحوّل المستخدم إلى مصدر غير مباشر لجمع بيانات أشخاص آخرين دون علمهم أو موافقتهم.

2. الاختراق:

يُعدّ الاختراق من أخطر التهديدات الأمنية التي تواجه أنظمة المعلومات والاتصالات، حيث يتمثل في الوصول غير المشروع أو غير المصرح به إلى نظم الحواسيب أو الشبكات أو قواعد البيانات بغرض التجسس أو السرقة أو التخريب. ويتم غالبًا من خلال استغلال الثغرات الأمنية في الأنظمة المستهدفة باستخدام أدوات وتقنيات متقدمة، وقد يكون ذلك للوصول إلى البيانات الحساسة، تعديلها، حذفها، أو حتى استخدامها في تنفيذ عمليات إلكترونية ضارة أخرى. ويُطلق على هذا النوع من الهجمات "هجمات الاختراق" (Penetration Attacks)، وهي من أكثر أساليب الهجوم تعقيدًا وتأثيرًا، حيث تسعى إلى كشف نقاط الضعف في البنية التحتية للمعلومات، واختراقها بهدف السيطرة عليها أو إلحاق الضرر بها. (جبور، 2018، ص 34)

وغالبًا ما تتم عمليات الاختراق من خلال نشر برمجيات خبيثة يتم تثبيتها خلسة في أجهزة المستخدمين، كأحصنة طروادة أو فيروسات أو برامج تجسس، مما يتيح للمهاجم الوصول

إلى معلومات حساسة مثل كلمات المرور، المعلومات البنكية، أو البيانات الشخصية. وقد يستخدم المهاجمون هذه الأجهزة لاحقًا كمنصات لتنفيذ هجمات على أهداف أكبر، مثل شبكات الشركات أو المؤسسات الحيوية.

3. برنامج السرقة Vidar:

يُعد برنامج Vidar من أبرز أدوات سرقة المعلومات، إذ يستهدف الأجهزة خلسة لجمع بيانات حساسة مثل بيانات النظام، معلومات تسجيل الدخول، بطاقات الائتمان، سجلات التصفح، ملفات تعريف الارتباط، المحافظ الرقمية، رسائل البريد الإلكتروني، وبيانات FTP. ويعود أصل Vidar إلى تطوير فيروس "حصان طروادة Arkei"، وتم توفيره منذ 2018 عبر مواقع الويب المظلم كخدمة مدفوعة.

يتميز Vidar باستخدامه للبنية التحتية للقيادة والتحكم (2C) من خلال منصات مثل Telegram وSteam وMastodon. ويتم تضمين عنوان IP لخادم القيادة في ملفات تعريف على هذه المنصات، مما يسمح للبرمجية بإرسال واستقبال الأوامر، تنزيل الملفات الضارة، أو تثبيت برمجيات إضافية.

يُنتشر Vidar عادةً عبر رسائل البريد الإلكتروني العشوائي، التي تحتوي على مرفقات ضارة مثل مستندات Office بوحدات ماكرو مفعلة، أو ملفات ISO، أو أرشيفات ZIP مزيفة، أو برامج تثبيت احتيالية لبرامج معروفة. وقد استخدم المهاجمون حتى إعلانات مزورة على محرك بحث Google لخداع المستخدمين لتحميل البرنامج الضار.

عند الإصابة، يجمع Vidar البيانات الحساسة، يعبئها في ملف ZIP، ويرسلها إلى الخادم ثم يحذف نفسه تلقائيًا لإخفاء آثاره. ويعتمد أيضًا على أساليب خداع متطورة، مثل تضخيم حجم الملفات للتخفي عن برامج مكافحة الفيروسات واستخدام شهادات رقمية منتهية الصلاحية.

إضافة إلى سرقة المعلومات، يمكن أن يستخدم Vidar لتوصيل برمجيات طلب الفدية مثل STOP/Djvu وGandCrab، مما يضاعف من خطورة الإصابة عبر جمع بيانات الضحية وابتزازه.

بسبب تطور وسائل انتشاره وصعوبة اكتشافه، يمثل Vidar تهديدًا كبيرًا للخصوصية الرقمية سواء للأفراد أو المؤسسات، مما يستدعي توخي الحذر عند التعامل مع المرفقات الإلكترونية ومصادر التحميل غير الموثوقة.

(https://me.kaspersky.com/resource-center/threats/vidar-stealer، 2025/04/28، 22:25.)

4. برامج الفدية:

تعد برامج الفدية تهديدًا خطيرًا، إذ تقوم هذه البرمجيات الضارة بإقفال الأجهزة أو تشفير ملفاتها وابتزاز الضحية لدفع فدية مقابل استعادة البيانات. تبدأ الإصابة عادةً بالحصول على وصول إلى الجهاز ثم تنفيذ عملية التشفير.

ظهر برنامج الفدية BlackCat منذ نوفمبر 2021، وأصبح من أكثر أنواع برامج الفدية تطورًا، حيث يعمل ضمن نموذج "برمجيات الفدية كخدمة" (RaaS). يتميز باستخدامه للغة البرمجة Rust، وقدرته على تنفيذ "الابتزاز الثلاثي"، من خلال تشفير البيانات، والتهديد بنشرها، وإمكانية تنفيذ هجمات حجب الخدمة (DDoS) إذا لم تُدفع الفدية.

يتيح BlackCat للمهاجمين تنفيذ هجماتهم عبر تخصيص خوارزميات التشفير، وكتابة ملاحظات الفدية، واختيار الملفات المستهدفة، وحتى استخدام بيانات اعتماد المجال لنشر العدوى عبر الشبكات. كما أن وجوده لا يقتصر على الويب المظلم، بل أنشأ موقعًا عامًا لتسريب البيانات، مما يضاعف الضغط على الضحايا.

ينتشر برنامج BlackCat عبر رسائل البريد الإلكتروني المصابة وروابط المواقع الضارة، مستهدفًا الأجهزة بنظامي Windows وLinux على حد سواء. ويمثل ملف التكوين القابل للتخصيص (JSON) أحد أهم أدواته، مما يزيد من مرونته في التنفيذ والانتشار.

الضحايا النموذجيون لـ BlackCat هم المؤسسات الكبيرة في قطاعات مختلفة كالرعاية الصحية، والطاقة، والخدمات اللوجستية، والتمويل. وتراوحت طلبات الفدية بين مئات الآلاف إلى ملايين الدولارات، تُطلب عادةً بعملة مشفرة مثل البيتكوين. ومن أمثلة هجمات BlackCat، ففي نوفمبر 2023 تعرضت شركة هنري شين لهجوم أسفر عن سرقة 35 تيرابايت من البيانات، وتم ابتزازها مع تهديد بنشر المعلومات، قبل أن يتم حذف البيانات لاحقًا بعد مفاوضات مع العصابة، وفي أغسطس 2023 استهدفت عصابة مجموعة سيكو وتم تسريب بيانات 60 ألف سجل، شملت معلومات عملاء وموظفين دون المساس ببيانات بطاقات الائتمان. واستجابت الشركة عبر تحسين أنظمتها الأمنية وتعزيز إجراءات الحماية.

https://me.kaspersky.com/resource-center/threats/blackcat-) ransomware، ، 2025/04/28، 22:40)

5. اصطياد البيانات الشخصية وتقنيات الكوكيزcookies

تقوم معظم مواقع الويب، عند زيارتها، بوضع ملف صغير يُعرف بـ"الكوكيز" على القرص الصلب الخاص بجهاز المستخدم، ويتصل هذا الملف بالخادم الخاص بالموقع الذي تتم زيارته عبر شبكة الإنترنت. يقوم الخادم بإرسال الكوكيز إلى جهاز المستخدم أثناء تصفحه لأي موقع إلكتروني، ويحتفظ بنسخة من هذه الرسائل لديه. ومن خلال هذه العملية، قد يتعرض المستخدمون لانتهاك خصوصيتهم وجمع معلومات عنهم خلال تصفحهم للمواقع، إذ تمكن الكوكيز المواقع من معرفة عنوان الإنترنت (IP) وطريقة الاتصال بالشبكة، إلى جانب المواقع التي تتم زيارتها، ونوع الجهاز والمعالج المستخدم، بالإضافة إلى البيانات الشخصية التي قد يُطلب من المستخدم إدخالها، مثل الاسم، البريد الإلكتروني، رقم البطاقة الائتمانية، العنوان، وغيرها من المعلومات الحساسة. (عثمان، ص 14)

تقوم معظم مواقع الويب، عند زيارتها، بتخزين ملف صغير يُعرف بـ"الكوكيز" على القرص الصلب الخاص بجهاز المستخدم، ويتصل هذا الملف بالخادم الخاص بالموقع عبر شبكة الإنترنت. يسمح الكوكيز بجمع معلومات عن المستخدم مثل عنوان الإنترنت (IP)، طريقة الاتصال، نوع الجهاز والمعالج، إضافة إلى بيانات حساسة مثل الاسم، البريد الإلكتروني، العنوان، ورقم البطاقة الائتمانية.

ويُعد استخدام الكوكيز جزءًا من تشريعات الخصوصية التي تلزم مواقع الإنترنت بالحصول على موافقة صريحة من المستخدمين قبل تخزين أو استرجاع أي معلومات على أجهزتهم. يهدف هذا الإجراء إلى حماية الخصوصية عبر الإنترنت، من خلال توعية المستخدمين بكيفية جمع معلوماتهم واستخدامها، ومنحهم خيار الموافقة أو الرفض

عادةً ما يظهر شريط تحذيري عند دخول الموقع، يعلم الزائر باستخدام ملفات الكوكيز ويطلب موافقته. وعلى الرغم من التزام عدد كبير من المواقع بهذه القوانين، إلا أن الدراسات، أشارت إلى أن كثيرًا من المستخدمين لا يتعاملون بفاعلية مع هذه الخيارات.

تُعرف ملفات الكوكيز بأنها ملفات نصية صغيرة يتم تكوينها تلقائيًا عند زيارة موقع إلكتروني، وتحتوي على بيانات شخصية تُستخدم لتحليل اهتمامات المستخدمين وتوجيه الإعلانات المناسبة لهم. وهي نوعان: ملفات طويلة المدى تبقى على الجهاز لفترات تمتد لأسابيع، وملفات قصيرة المدى تستمر لدقائق محدودة. وتُعد هذه الملفات عرضة للوصول غير المشروع من قبل مواقع أخرى، مما يُعرض خصوصية المستخدمين للانتهاك.

- ويتم تتبع المستخدمين من قبل متتبعي الطرف الثالث Third-Party Trackersعندما يقوم المستخدم بزيارة موقع إلكتروني، يُعتبر هذا الموقع طرفًا أولًا لتقديم الخدمة والتفاعل المباشر مع المستخدم، الذي يُعد الطرف الثاني. ومع ذلك، غالبًا ما يغفل المستخدمون عن وجود طرف ثالث يقوم بجمع بياناتهم دون علمهم المباشر. يشير تتبع الطرف الثالث إلى قيام مواقع لم يزرها المستخدم صراحةً بتتبع نشاطه وجمع معلوماته.

ورغم إدراك بعض المستخدمين لاحتمالية جمع معلوماتهم عبر الإنترنت، إلا أن الوعي بتتبع الطرف الثالث ومخاطره على الخصوصية يظل محدودًا، فتقوم شركات الطرف الثالث بزرع ملفات تعريف ارتباط (Cookies) عبر مختلف المواقع التي يزورها المستخدم، مما يسمح بجمع معلومات حول نشاطه عبر الإنترنت، غالبًا لأغراض إعلانية. ويظهر هذا النوع من التتبع جليًا عندما يلاحق إعلان معين المستخدم أثناء تنقله بين مواقع مختلفة. ومن أبرز شركات تتبع الطرف الثالث: DoubleClick وAmazon Ad System و Cambridge Analytica.

علاوة على ذلك، يمكن إنشاء ملف تعريف فريد للمستخدم دون الحاجة إلى ملفات تعريف ارتباط تقليدية، عن طريق تجميع بيانات فنية حول جهازه، مثل إصدار المتصفح ونظام التشغيل والخطوط المثبتة، مما يُعرف بـ"بصمة الجهاز" (Fingerprint)، والتي تتيح تتبع نشاط الجهاز عبر الإنترنت. كما أن متتبعي الطرف الثالث يستخدمون تقنيات خفية ومتطورة، مما يصعب على المستخدمين حماية أنفسهم من هذه الأساليب. (البوراصي، 2022، ص02)

6. البريد الإلكتروني:

يُعتبر البريد الإلكتروني أحد أهم المداخل إلى العالم الرقمي الشخصي، إذ تعتمد عليه معظم المواقع الإلكترونية، سواء للتسجيل أو لإدارة حسابات المستخدمين. تطلب العديد من منصات التسوق الإلكتروني والبنوك والمواقع الخدمية تسجيل البريد الإلكتروني، بهدف إرسال تحديثات الأسعار أو العروض أو الإعلانات. إلا أن بعض هذه المواقع قد تلجأ إلى أساليب خفية وغير قانونية للحصول على قوائم البريد الإلكتروني للأصدقاء والمعارف، بهدف استغلالها لاحقًا لأغراض تسويقية.

وتُعد رسائل التصيد الاحتيالي من أبرز التهديدات المرتبطة بالبريد الإلكتروني، حيث تحتوي هذه الرسائل على روابط أو مرفقات خبيثة مصممة لاختراق أنظمة المستخدمين وسرقة بياناتهم الحساسة مثل كلمات المرور، أرقام الحسابات المصرفية، أو بيانات الهوية. وغالبًا

ما يتنكر المهاجمون في هيئة كيانات موثوقة كالشركات الكبرى أو المؤسسات الحكومية لخداع الضحايا.

بالإضافة إلى ذلك، يلجأ المخترقون إلى "انتحال البريد الإلكتروني" بإنشاء عناوين إلكترونية مزيفة تحاكي عناوين المستخدمين مع تغييرات طفيفة، مما يسمح لهم بخداع معارف المستخدم وجمع معلومات إضافية منهم. اختراق حساب البريد الإلكتروني يُمكن أن يؤدي إلى الوصول إلى حسابات أخرى مرتبطة به، مما يسهل عملية انتحال الهوية الرقمية أو ارتكاب جرائم مالية.

تُستخدم أدوات البحث العكسي ومحركات البحث على الإنترنت في تتبع معلومات المستخدمين عبر بريدهم الإلكتروني، مما يسهل على المهاجمين جمع معلومات شخصية إضافية كالموقع الجغرافي، العمل، الحسابات الاجتماعية، وأحيانًا معلومات مالية. كما أن ارتباط البريد الإلكتروني بحسابات وسائل التواصل الاجتماعي يزيد من حجم المعلومات المعرضة للخطر.

ولا يقتصر التهديد على الأفراد فقط، بل يمتد إلى الشركات والمؤسسات الكبرى، حيث يؤدي اختراق حسابات البريد الإلكتروني إلى خروقات كبيرة للبيانات، مكلفة جدًا من الناحية الاقتصادية.

من جهة أخرى، يشكل البريد العشوائي (Spam) خطرًا إضافيًا، حيث يتم إرسال كميات ضخمة من الرسائل بغرض الإغراق المعلوماتي، أو الترويج لعروض وهمية، أو نشر برمجيات خبيثة بهدف التجسس أو سرقة البيانات.

(https://me.kaspersky.com/resource-center/threats/hackers-and-email-addresses ، 2025/04/28، 23:20)

7. الاعتداء على الملكية الفكرية لأسماء مواقع الإنترنت:

تُعد الاعتداءات على الأسماء الثابتة للمواقع الإلكترونية من أبرز أشكال التعدي المنتشرة عبر شبكة الإنترنت، حيث يتمثل هذا النوع من الاعتداء في استخدام أسماء نطاقات

(Domain Names) تتطابق أو تتشابه مع أسماء مواقع شهيرة، بهدف خداع المستخدمين وتحويلهم إلى مواقع أخرى، في عملية تُعرف بـ"إعادة التوجيه" (Redirection)، والتي تُصنف ضمن الجرائم الإلكترونية الشائعة.

وقد وقعت حادثة بارزة عام 1999، حين تمكن بعض المخترقين من اختراق نظام تسجيل أسماء النطاقات الخاص بشركة "نايك" (Nike)، من خلال شركة " Network Solutions"، وأعادوا توجيه زوار الموقع الرسمي إلى مواقع أخرى بغرض سرقة البيانات أو نشر رسائل معينة. (محمد، 2016، ص 17-13.)

8. احتيال تبديل بطاقة SIM:

أصبح احتيال تبديل بطاقة SIM مصدر قلق متزايد، خاصة في الولايات المتحدة ودول أخرى تشهد انتشارًا واسعًا للهواتف الذكية. ويحدث هذا الاحتيال عندما يتمكن محتال من السيطرة على رقم هاتف الضحية عبر إقناع شركة الهاتف بنقل الرقم إلى بطاقة SIM جديدة بحوزته، مما يمكنه من الاستيلاء على المكالمات، الرسائل النصية، ورموز المصادقة، وبالتالي السيطرة على الحسابات البنكية وملفات تعريف وسائل التواصل الاجتماعي.

تبدأ العملية بجمع المهاجم معلومات شخصية عن الضحية عبر التصيد الاحتيالي أو شراء البيانات من السوق السوداء، ثم يستخدمها لانتحال هوية الضحية أمام مزود الخدمة. بمجرد نقل الرقم، يصبح الجهاز الأصلي بلا خدمة، بينما يتمكن المهاجم من الدخول إلى حسابات الضحية الحساسة.

وتشير تقارير مكتب التحقيقات الفيدرالي إلى أن خسائر احتيال تبديل بطاقة SIM بلغت 68 مليون دولار أمريكي عام 2021، مقارنة بـ 12 مليون دولار خلال الفترة 2018-2020، مما يعكس خطورة هذه الظاهرة. أحيانًا، قد يساعد موظفون لدى شركات الاتصالات في تنفيذ الهجوم بشكل مباشر ومن علامات احتيال تبديل بطاقة SIM ما يلي:

- استقبال إشعارات غريبة بشأن تغيير الخدمة.
- فقدان مفاجئ لخدمة الاتصال أو البيانات.

- منشورات غير معتادة على حسابات وسائل التواصل الاجتماعي.
- قفل الحسابات البنكية أو البريد الإلكتروني فجأة.
- ظهور معاملات مالية مشبوهة على الحسابات المرتبطة بالهاتف.
- يعد وعي المستخدم بالمؤشرات المبكرة والتواصل السريع مع مزود الخدمة أمرًا أساسيًا للتقليل من الأضرار الناتجة عن هذا النوع من الهجمات.

(https://me.kaspersky.com/resource-center/threats/sim-swapping، 2025/04/28، 22:50 ،)

9. أدوات ومواقع جمع البيانات وتحليلها:

تقدّم بعض الشركات خدمات خاصة لمواقع التسوق ومواقع الأخبار والمواقع التي تهتم بجمع بيانات المستخدمين، حيث تتولى هذه الشركات مسؤولية تتبع جميع تحركات المستخدم داخل الموقع الإلكتروني. وتشمل هذه العملية تسجيل سلوك المستخدم، الروابط التي ينقر عليها، وحتى تسجيل نقرات الماوس والنصوص المكتوبة، بالإضافة إلى تسجيلات فيديو لحركة المستخدم أثناء تصفحه.

تُستخدم هذه البيانات لاحقًا لتحليل سلوك الزوار واتخاذ القرارات المناسبة بناءً على طبيعة الموقع وأهدافه. ومن أشهر المنصات التي تقدم مثل هذه الخدمات موقع Hotjar، الذي يعد حلاً متكاملاً لتحليلات مواقع الويب. يشمل Hotjar إنشاء خرائط حرارية (Heatmaps) لسلوك المستخدم، وتسجيلات للجلسات تتبع حركة الماوس، وتحليل مسارات التحويل، بالإضافة إلى استطلاعات الرأي والاستطلاعات الكاملة التي تُسجل نقرات الماوس ومختلف تفاعلات المستخدم مع الموقع. (الدوكالي، 2022، ص 03)

10. غرف الدردشة والمحادثات في الفضاء الإلكتروني:

أصبح العديد من المستخدمين يلجؤون إلى ما يُعرف بغرف الدردشة (Chat Rooms) داخل الفضاء الإلكتروني (Cyber Space) بهدف التفاعل أو التسلية أو حتى بناء

علاقات افتراضية. ويُلاحظ أن بعض هذه المحادثات قد تفتقر إلى الخصوصية، خاصة حين تُدار عبر منصات عامة تتيح لأي مستخدم الانضمام والتفاعل مع الآخرين.

وتُظهر الدراسات أن هذه المحادثات، التي قد تبدأ بنقاشات عادية، سرعان ما تتطور إلى تبادل للبيانات الشخصية، مثل البريد الإلكتروني، دون إدراك حقيقي لمخاطر استخدام هذه المعلومات. وفي كثير من الأحيان، يتم استغلال غرف الدردشة كوسيلة للإيقاع بالضحايا، خصوصًا من فئة الشباب، من خلال التواصل الزائف أو الاحتيال الرقمي. (امين، جرائم الحاسوب والانترنيت – الجريمة المعلوماتية، 2007، ص 45)

11. التنصت على الآخرين:

يتنصت المجرم الالكتروني على الحياة الخاصة بالآخرين عن طريق استخدام برنامج معين يقوم بفتح منفذ في جهاز الشخص المعتدي عليه، يمكن من خلاله الاطلاع والاستماع إلى جميع المحادثات والمراسلات الصادرة من الشخص المعتدى عليه ويتم إدخال هذا الملف إلى الجهاز المعتدى عليه عن طريق البريد الالكتروني أو عن طريق مواقع مغرية يزورها المعتدى عليه.

12. **التشهير:**

التشهير وتشويه السمعة في مواقع التواصل الاجتماعي سهل وميسر للعابثين وذلك بالقيام بنشر معلومات حصل عليها المتصل بطريقة غير مشروعة أو معلومات مغلوطة وتهدف الى كسب مادي أو سياسي أو اجتماعي معين.

13. **برامج الدعاية وبرامج التجسس (Ad ware and Spy ware):** تُعد برامج الدعاية وبرامج التجسس من أكثر الوسائل الخفية التي تُستخدم لاختراق خصوصية المستخدمين دون علمهم. وغالبًا ما يتم إدخال هذه البرامج إلى أجهزة المستخدمين بطرق ملتوية، من أبرزها دمجها مع برامج تبدو غير ضارة أو مجانية، بحيث يتم تثبيتها تلقائيًا عند تحميل البرنامج الرئيسي. وبمجرد تنصيبها على الجهاز، تبدأ هذه البرامج في العمل بشكل غير مرئي، حيث تقوم بجمع كمٍّ هائل من المعلومات الخاصة بالمستخدمين.

تعتمد هذه البرامج في نشاطها على تحليل بقايا ملفات تعريف الارتباط (Cookies) المتروكة على الجهاز، كما أنها تبحث داخل النظام عن أي بيانات شخصية أو سلوكية يمكن استغلالها، كالتفصيلات في التصفح، الكلمات المفتاحية المستخدمة، والبرامج الأكثر استخدامًا. ومن خلال هذه البيانات، يتم إنشاء ملف شخصي عن كل مستخدم، يُرسل لاحقًا إلى جهات متعددة، مثل شركات التسويق، أو مواقع التسوق الإلكتروني، أو شركات تحليل البيانات، التي تستغلها لأغراض دعائية وتجارية أو حتى سياسية في بعض الأحيان.

ويمثل هذا النوع من البرمجيات تهديدًا صامتًا لأمن المعلومات، إذ لا يقتصر ضرره على الإعلانات المزعجة، بل يتعداه إلى المساس بالخصوصية الفردية وتسهيل الوصول غير المصرح به إلى بيانات قد تكون حساسة للغاية. كما أن استمرار وجود هذه البرامج على الجهاز قد يؤدي إلى بطء الأداء، وتعطيل بعض الوظائف، وزيادة قابلية الجهاز للاختراق من قبل برامج ضارة أخرى. (الدوكالي، 2022، ص 03)

3.3. أساليب الحكومات في انتهاك الخصوصية الرقمية:

لقد أصبح انتهاك حقوق الأفراد في التمتع بالحياة الخاصة وعدم احترام خصوصياتهم ظاهرة متفشية خلال فترة الحرب الباردة، خاصة في الدول ذات الأنظمة السياسية المغلقة. فقد كانت هذه الدول، من خلال أجهزتها الأمنية، تتخذ إجراءات احترازية ضد أي تحركات أو أفكار تتعلق بالحريات السياسية أو مطالب التغيير السياسي وتداول السلطة. وكانت ترى أن انتهاك خصوصيات الأفراد إجراء استباقي ضروري تبرره الاحتياجات الأمنية للدولة.

وكان الاعتقاد السائد أن الدول الأخرى، التي تختلف عن الدول الاستبدادية، توفر مجالًا واسعًا للحريات وتحترم خصوصية الأفراد، مستندة في ذلك إلى مجموعة من التشريعات والقوانين وحرية الإعلام في فضح الانتهاكات التي قد تطال تلك الخصوصية والحرية الشخصية، والتي تحظى بتقدير عالٍ. غير أن السنوات الأخيرة كشفت عن حقائق صادمة بشأن مدى احترام الخصوصيات المتعلقة بالمواطنين والمقيمين في دول الغرب،

حيث يتم التنصت على الاتصالات والتجسس على الملفات الشخصية وقرصنة المعلومات، وكل ذلك تحت مبرر الدواعي الأمنية ومكافحة الإرهاب.

تأتي الولايات المتحدة الأمريكية في مقدمة الدول التي تمارس هذه الانتهاكات للخصوصية، خاصة منذ أحداث 11 سبتمبر 2001. فقد أصبحت هيمنتها على منظومة الاتصالات والمعلوماتية العالمية واضحة، مما يمكنها من الوصول إلى بيانات ومعلومات ملايين المستخدمين للتكنولوجيا الحديثة. كما تمتلك القدرة على تفعيل نظم المراقبة والتصوير والتجسس التي تطال ملايين الأفراد في مختلف أنحاء العالم. وفي هذا السياق، كشف إدوارد سنودن، الموظف السابق لدى وكالة المخابرات المركزية الأمريكية والمقيم حالياً في روسيا، عن معلومات تفيد بأن وكالة الأمن القومي في الولايات المتحدة ومقر الاتصالات العامة في بريطانيا طوّرا معاً تكنولوجيات تسمح بالوصول إلى الكثير من حركة الإنترنت العالمية، وسجلات المكالمات، ودفاتر العناوين الإلكترونية للأفراد، وأحجام هائلة من محتوى الاتصالات الرقمية الأخرى.

وفي السياق ذاته، أظهرت التقارير أن السلطات الأسترالية قامت باختراق سجلات المواقع الإلكترونية الأسترالية في عام 2015 بواسطة مزودي خدمة الإنترنت في أستراليا للوصول إلى معلومات تتعلق بالأفراد. أما في الصين، فهناك برنامج معلن عنه لهذه الغايات يُطلق عليه "مشروع الدرع الذهبي" (Golden Shield Project)، وهو برنامج مخصص لمراقبة الأفراد ضمن وزارة الأمن القومي الصينية، حيث اعتمد في عام 1998 وبدأ العمل فيه في عام 2003.

يجب أن نسجل في هذا الإطار ملاحظة متعلقة بمسألة الوصول إلى المعلومات السرية وتضرر أصحابها من هذا الفعل. ففي الماضي، كان الضغط أكثر نحو مطالبة الحكومات بحماية خصوصية الأفراد، وضمان وجود قانون واضح وفعّال لتأمين ذلك، ومتابعة من ينتهك تلك الخصوصية، باعتبار أن ذلك أحد واجباتها. إلا أن حدة التطور العلمي في مجال الاتصالات، خاصة، جعلت الحكومات نفسها عاجزة عن تحصين معلوماتها وبياناتها، حتى

السرية منها. وهذا يثير التساؤل بشأن الجهة والتقنية القادرة على توفير ذلك، والآليات القانونية التي تمكّن ضحايا انتهاك الخصوصية من التعويض عن الضرر الذي لحقهم جراء ذلك. (الرزي، عام 2017، ص 3)

4.3. آليات حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي.

1. الحماية على مواقع التواصل الاجتماعي:

تُعدّ مراجعة إعدادات الخصوصية في شبكات التواصل الاجتماعي ضرورة أساسية لتعزيز حماية البيانات الشخصية للمستخدمين. إذ تتيح هذه المراجعة إمكانية التحكم في من يمكنه الوصول إلى المحتوى المنشور والمعلومات الشخصية، إلى جانب الحد من تعقب الأنشطة الرقمية وتقليل الإعلانات الموجهة. ومن الضروري الإلمام بسياسات الخصوصية المعتمدة في كل منصة رقمية، ومدى مشاركتها للبيانات مع أطراف خارجية، فضلاً عن تفعيل الإشعارات والتنبيهات لرصد الأنشطة غير المصرح بها.

إن الإفراط في مشاركة المعلومات الشخصية عبر الإنترنت يشكل تهديدًا مباشرًا للخصوصية الرقمية، حيث يُمكن للمخترقين أو الجهات الخبيثة تجميع البيانات الشخصية واستغلالها في أنشطة احتيالية. ومن الإجراءات الوقائية المهمة الامتناع عن نشر تفاصيل متعلقة بالحياة اليومية كخطط السفر أو معلومات الإقامة، مع مراعاة تأجيل نشر صور الرحلات إلى ما بعد العودة، لتفادي كشف معلومات قد تُستغل ضد المستخدمين.

كما يُنصح بتعطيل خاصية تحديد الموقع الجغرافي المرتبطة بالمحتوى المنشور، وتجنّب التفاعل مع التطبيقات أو الاختبارات التي تطلب معلومات تُستخدم عادة كإجابات لأسئلة الأمان، مثل أسماء المدارس أو الحيوانات الأليفة. بالإضافة إلى ذلك، ينبغي توخّي الحذر عند التعامل مع المسابقات والعروض الترويجية، إذ إن كثيرًا منها يُستخدم كوسيلة لنشر برمجيات ضارة أو لجمع بيانات المستخدمين بطرق غير مشروعة.

ويُوصى كذلك بأن يُضبط الملف الشخصي على الوضع "الخاص"، بحيث تقتصر إمكانية الوصول إلى البيانات الشخصية على الأفراد الموثوقين فقط. كما يُحظر استخدام

منصات التواصل في تبادل المعلومات الحساسة، كصور جوازات السفر أو بطاقات الهوية، لما لذلك من مخاطر ترتبط بإمكانية الوصول غير المصرح به من جهات متعددة.

وفيما يخص تبادل البيانات الشخصية والملفات الحساسة، يُفضل استخدام تقنيات التشفير عند إرسالها (مثل ملفات PDF أو ZIP المحمية بكلمة مرور)، على أن تُرسل كلمة المرور عبر قناة اتصال منفصلة، لضمان أقصى درجات الأمان.

ومن المعلوم أن عمليات الاحتيال الإلكتروني منتشرة بشكل واسع على منصات التواصل، حيث يعتمد المحتالون على انتحال شخصيات أصدقاء أو جهات موثوقة، باستخدام رسائل وهمية وروابط خبيثة تستهدف سرقة بيانات الدخول أو الأموال.

(https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/stay-safe-on-social-media/ ، 2025/05/03، 17:00.)

- استخدام كلمات مرور قوية وفريدة لا تُستخدم في أكثر من حساب.
- تفعيل خاصية التحقق بخطوتين (SV 2) لتعزيز أمان الحسابات.
- تقييد إعدادات الخصوصية على منصات التواصل بحيث لا يتمكن من رؤية المنشورات سوى الأشخاص المصرّح لهم.
- الامتناع عن قبول طلبات الصداقة أو المتابعة من أشخاص غير معروفين.

2. تحسين أمان كلمة المرور:

في ظل تزايد التهديدات والاعتماد المتنامي على الخدمات الرقمية، باتت كلمات المرور تمثل خط الدفاع الأول في حماية البيانات الشخصية والمصرفية، مما يفرض ضرورة اتباع ممارسات مدروسة تعزز من أمان الحسابات. ومن أبرز هذه الممارسات إنشاء كلمات مرور قوية باستخدام ثلاث كلمات عشوائية غير مترابطة، مثل "CactusBicyclePants" أو "MoonBellowGiraffe"، مع إمكانية تعزيزها بإدخال أرقام أو رموز حسب متطلبات الموقع. وتُعد هذه الطريقة فعّالة في مواجهة محاولات الاختراق، بشرط تجنب استخدام

معلومات شخصية شائعة أو كلمات مرور مكررة. كما يُنصح باستخدام مديري كلمات المرور الذين يوفرون أدوات لتوليد كلمات مرور معقدة وتخزينها بشكل مشفر وآمن، مما يقلل الحاجة لتذكر العديد من الكلمات المعقدة ويضمن حماية المعلومات من الوصول غير المصرح به. ويُفضل اختيار كلمة مرور رئيسية قوية لمدير كلمات المرور، وتفعيل المصادقة الثنائية لحماية إضافية. من جهة أخرى، ينبغي تغيير كلمات المرور الافتراضية على الأجهزة الذكية المنزلية مثل أجهزة التلفاز وأجهزة التحكم في الحرارة، حيث غالبًا ما تكون هذه الإعدادات ضعيفة ومعروفة مسبقًا، مما يسهل اختراقها. ومن المهم أيضًا تجنّب حفظ كلمات المرور على أجهزة العمل، لا سيما أن ذلك قد يعرّض البيانات الشخصية للوصول غير المصرّح به من قبل فريق الدعم أو في حال اختراق الشبكة المؤسسية. إن تبني هذه الإجراءات، إلى جانب التحديث المستمر لكلمات المرور والتوعية بمخاطر إعادة استخدامها، يساهم بشكل كبير في بناء بيئة رقمية أكثر أمانًا.

https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-)
،./fraud/protecting-against-online-fraud/stay-safe-on-social-media
(17:00 ،2025/05/03

3. التعرف على رسائل البريد الإلكتروني والروابط الاحتيالية.

إذا تمكّن أحدهم من اختراق حساب بريدك الإلكتروني، فقد يتمكن من الوصول إلى حساباتك الأخرى عبر الإنترنت من خلال استغلال ميزة "نسيت كلمة المرور"، أو قد يحصل على معلومات شخصية يستخدمها لاحقًا في محاولات احتيال ضدك أو ضد معارفك. لهذا السبب، من الضروري أن تستخدم دائمًا كلمة مرور قوية وفريدة لحساب بريدك الإلكتروني، ومن الأفضل اعتماد نفس النهج مع حساباتك الأخرى، مثل حسابات وسائل التواصل الاجتماعي ومواقع التسوق الإلكتروني، لتقليل مخاطر الاختراق المتسلسل. ففي حال تم اختراق أحد الحسابات، لن يتمكن المجرم من الوصول إلى بقية الحسابات باستخدام نفس كلمة المرور.

أما فيما يتعلق بالتعرف على رسائل البريد الإلكتروني والروابط الاحتيالية، فهناك عدة مؤشرات يمكن من خلالها التحقق من موثوقية الرسالة. من المهم فحص عنوان البريد الإلكتروني بدقة، إذ قد يبدو مشابهًا لعناوين حقيقية لكنه يحتوي على تغييرات طفيفة أو أخطاء إملائية تشير إلى احتيال. كما يجب الانتباه إلى استخدام رموز وأحرف غير مألوفة في العنوان، والتحقق من صياغة الرسالة من حيث اللغة والنحو، حيث إن رسائل الاحتيال غالبًا ما تكون ركيكة أو مليئة بالأخطاء. يُنصح بعدم النقر المباشر على الروابط، وبدلاً من ذلك كتابة عنوان الموقع يدويًا لتجنب التوجيه إلى صفحات مزيفة. كما ينبغي فحص اسم المرسل، فقد يستخدم المحتالون أسماء مشابهة لأسماء شركات معروفة. تجنّب التفاعل مع الرسائل التي تحثك على اتخاذ إجراءات عاجلة أو تطلب معلومات شخصية أو مالية، فهذه أساليب ضغط نفسي يستخدمها المجرمون. احذر كذلك من فتح الملفات المرفقة إذا لم تكن متأكدًا من مصدرها، فقد تكون محملة ببرمجيات خبيثة. استفد من خاصية المعاينة التي توفرها بعض برامج البريد الإلكتروني لمعرفة محتوى الرابط قبل فتحه. وأخيرًا، لا تتفاعل مع الرسائل غير المتوقعة من جهات مجهولة، واستشر المصادر الرسمية من خلال مواقع الشركات أو الجهات المعنية للتحقق من مصداقية الرسالة. إتباع هذه الإرشادات يُسهم في تعزيز الأمان الرقمي والحد من مخاطر الاحتيال عبر البريد الإلكتروني.

https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-)
(17:00 ،2025/05/03 ،/to-spot-postal-fraud

4. الاستفادة من شبكات VPN لتشفير بيانات التصفح:

تُعدّ شبكات (VPN شبكات الخصوصية الظاهرة) أداة فعالة لتعزيز أمان التصفح على الإنترنت، إذ توفر طبقة حماية إضافية من خلال تشفير بيانات المستخدم وإخفاء عنوان IP الخاص به، مما يقلل من فرص تعقب نشاطه أو اختراق اتصالاته. فعند استخدام VPN، يتم تشفير جميع البيانات المتبادلة بين جهاز المستخدم وخادم الشبكة، ما يصعّب على

المتطفلين أو المتسللين اعتراض المعلومات أو قراءتها. كما تتيح هذه الشبكات للمستخدمين إخفاء موقعهم الجغرافي الحقيقي عن المواقع والخدمات الإلكترونية، إذ يتم استبدال عنوان IP الخاص بهم بعنوان تابع لخادم VPN، مما يساعد في حماية الهوية الرقمية وتجاوز القيود الجغرافية على بعض المحتويات المحجوبة. وتُعدّ هذه الخاصية مفيدة بشكل خاص أثناء استخدام شبكات Wi-Fi العامة التي تُعد أكثر عرضة للاختراق، إذ تتيح VPN للمستخدم تأمين اتصاله ومنع أي نشاط تجسسي. كما تُسهم VPN في تقليل قدرة مواقع الويب والشركات على تتبع نشاط المستخدم عبر الإنترنت من خلال تعطيل أدوات التتبع مثل الكوكيز.

وعند التفكير في اختيار خدمة VPN موثوقة وآمنة، يجب الانتباه لعدة عوامل حاسمة. أولها التحقق من سجل الخدمة وسياسة الخصوصية الخاصة بها، مع ضرورة التأكد من تبنيها لسياسة "عدم تسجيل البيانات"، مما يعني أنها لا تحتفظ بأي معلومات عن نشاط المستخدم. من المهم أيضًا التأكد من استخدام الخدمة لتقنيات تشفير قوية مثل OpenVPN أو IKEv2/IPsec لضمان أعلى درجات الأمان. يُفضل كذلك اختيار خدمة VPN توفر خوادم متعددة في مناطق جغرافية متنوعة، مما يتيح للمستخدمين مرونة في الوصول إلى المحتويات المختلفة. سرعة الاتصال تُعدّ عاملاً مهمًا، خاصةً لأولئك الذين يستخدمون VPN في بث الفيديوهات أو لعب الألعاب عبر الإنترنت. كما يجب الانتباه إلى جودة دعم العملاء وتوافر المساعدة التقنية عند الحاجة، بالإضافة إلى مراجعة تجارب المستخدمين السابقين لتقييم جودة الخدمة من واقع الاستخدام. وأخيرًا، يجب النظر في العروض والأسعار دون جعل السعر هو العامل الأساسي، فبعض الخدمات المدفوعة قد توفر حماية وموثوقية أعلى، كما يُفضل تجربة الخدمة من خلال فترة تجريبية أو ضمان استرداد الأموال قبل الالتزام بالاشتراك. بهذا الشكل، يمكن للمستخدم حماية خصوصيته وتعزيز أمانه الرقمي بثقة وكفاءة. (https://me.kaspersky.com/resource-center/preemptive-

safety/how-to-protect-personal-online-privacy ، 2025/05/03، (17:30

5. إدارة ملفات تعريف الارتباط (الكوكيز):

إدارة ملفات تعريف الارتباط (الكوكيز) تُعد جزءًا أساسيًا من تجربة تصفح الإنترنت، حيث تعمل هذه الملفات على تخزين معلومات محددة حول تفضيلات ونشاطات المستخدمين على المواقع. يمكن للمستخدمين إدارة ملفات تعريف الارتباط من خلال إعدادات المتصفح، حيث يمكنهم حذف الكوكيز المخزنة، أو تعطيلها بشكل كامل، أو تحديد الكوكيز التي يسمحون بتخزينها. هذا يمنح المستخدمين سيطرة أكبر على خصوصيتهم على الإنترنت، والقدرة على تخصيص تجربتهم وتحسين أمان تصفحهم وتجنب التتبع غير المرغوب فيه. تُعتبر ملفات تعريف الارتباط ملفات صغيرة تُخزنها المتصفحات على جهاز الكمبيوتر عند زيارة موقع ويب معين، وتهدف إلى تخزين معلومات تتعلق بتفضيلات المستخدم ونشاطاته على الإنترنت، مما يمكن المواقع من تقديم تجربة أفضل وأكثر تخصيصًا. عند زيارة موقع ويب يحتوي على ملفات تعريف الارتباط، يتم إرسال البيانات من الموقع إلى جهاز الكمبيوتر وتخزينها هناك، وتشمل هذه البيانات معلومات مثل تفضيلات اللغة وتفاصيل تسجيل الدخول ومعلومات أخرى تعتمد على ما يقدمه الموقع. ما يتم تجميعه من بيانات يعتمد على نوع وهدف الموقع، حيث أن بعض ملفات تعريف الارتباط تجمع معلومات تفصيلية عن تفاعلات المستخدم مع الموقع مثل الصفحات التي زارها والمنتجات التي اشتراها أو عمليات البحث التي قام بها، وتُستخدم هذه المعلومات لتحسين تجربة المستخدم وتقديم محتوى مستهدف. من الجدير بالذكر أن ملفات تعريف الارتباط يمكن أن تكون جزءًا من تتبع الإعلانات، حيث تسمح للشركات الإعلانية بتقديم إعلانات مستهدفة استنادًا إلى اهتمامات المستخدم ونشاطاته على الإنترنت. للحفاظ على الخصوصية، يجب على المستخدمين التحكم في كيفية تفاعلهم مع ملفات تعريف الارتباط من خلال إعدادات المتصفح، حيث أن بعض المواقع قد تتطلب موافقة المستخدم على استخدام ملفات تعريف

الارتباط قبل السماح بالوصول إلى محتواها. لتقليل التتبع عبر الويب وزيادة الخصوصية من خلال إدارة ملفات تعريف الارتباط، يُنصح بحذف ملفات تعريف الارتباط بانتظام من المتصفح، واستخدام وضع التصفح الخاص الذي يمنع تخزين ملفات تعريف الارتباط والبيانات التصفحية، ومنع ملفات تعريف الارتباط من المواقع غير الموثوقة، وتعطيل ملفات تعريف الارتباط بشكل كلي إذا لزم الأمر، واستخدام ملحقات المتصفح لحجب الإعلانات والتتبع مثل AdBlock Plus وPrivacy Badger وuBlock Origin، واستخدام متصفحات متخصصة في الخصوصية مثل Brave وFirefox Focus وTor Browser، والتحقق من سياسات الخصوصية للمواقع قبل تقديم معلومات شخصية.

6. مراجعة أذونات حسابك وتقييد الوصول إلى التطبيقات الخارجية:

ينبغي على مستخدمي وسائل التواصل الاجتماعي توخي الحذر قبل منح أي تطبيق تابع لجهة خارجية إذن الوصول إلى حساباتهم، حيث تُطوَّر هذه التطبيقات من قبل مطورين خارجيين لتتكامل مع منصات التواصل الاجتماعي. ورغم أن هذه التطبيقات قد تضيف مزايا ممتعة، إلا أنها قد تُعرّض خصوصية بياناتك لمخاطر كبيرة، إذ إن منحها الإذن يعني السماح لها بالوصول إلى معلوماتك واستخدامها وجمعها من حسابك، مما يعني أنه في حال اختراق التطبيق، فإن المخترق سيحصل أيضًا على إمكانية الوصول إلى الحسابات المرتبطة به. لذلك، ولتعزيز حماية الخصوصية، يُنصح بالتحقق بانتظام من قائمة التطبيقات المرتبطة بحسابك على المنصة وإلغاء أذونات الوصول غير الضرورية.

https://me.kaspersky.com/resource-center/preemptive-)
(17:30 ،2025/05/03،safety/how-to-protect-personal-online-privacy

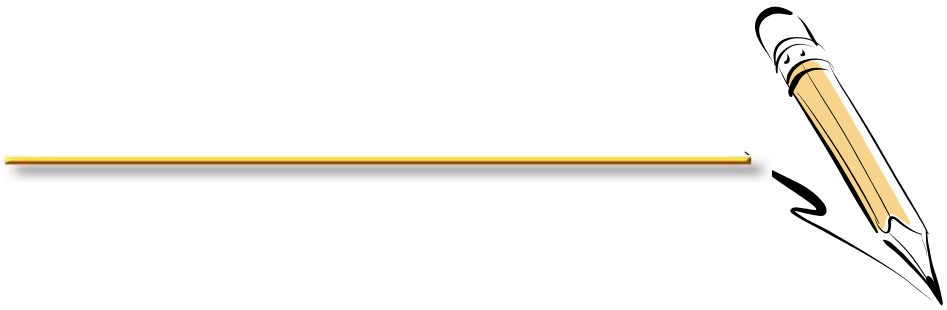
7. إيقاف تشغيل بيانات الموقع:

تُعتبر بيانات الموقع، وعلامات الموقع الجغرافي، وتسجيلات الدخول على مواقع التواصل الاجتماعي من المؤشرات التي يمكن أن تكشف عن موقعك الدقيق في لحظة معينة. وعند مشاركة هذه البيانات، فإنك تكشف للآخرين عن مكان وجودك أو غيابك، مما

يُعرّض سلامتك وسلامة أفراد عائلتك للخطر، ويزيد من احتمال تعرّضك للاعتداء الجسدي أو السرقة. حتى دون الإشارة المباشرة إلى موقعك، فإن الصور أو النصوص المنشورة قد تحتوي على تفاصيل تُستخدم لتحديد موقعك، مثل مشاركة فيديوهات منتظمة من حدث أسبوعي، مما يسمح بتتبع روتينك أو موقع تواجد أطفالك ومدارسهم. لذا، يُنصح مستخدمو مواقع التواصل الاجتماعي الساعون لحماية خصوصيتهم بعدم نشر الصور أو المعلومات المتعلقة بموقعهم إلا بعد انتهاء الحدث أو العودة من الرحلة، وتجنّب مشاركة أي تفاصيل تحدد الموقع بشكل مباشر أو غير مباشر.

8. برنامج مكافحة الفيروسات:

غالبًا ما يتضمن نظاما التشغيل ويندوز وآبل برنامج مكافحة فيروسات مدمج ومجاني، لذا فإن تفعيله يمنحك طبقة حماية فورية وفعالة ضد البرمجيات الخبيثة. أما بالنسبة للهواتف والأجهزة اللوحية، فلست بحاجة إلى برامج مكافحة فيروسات إضافية ما دمت تلتزم بتثبيت التطبيقات من المتاجر الرسمية مثل Google Play وApple App Store، حيث تقوم هذه المتاجر بإجراء فحوصات دقيقة للتأكد من خلو التطبيقات من الفيروسات أو أي برمجيات ضارة. ولتعزيز الأمان، يُنصح بضبط الجهاز والتطبيقات لتحديث نفسها تلقائيًا. كما يجب تطبيق التحديثات فور توفرها، إذ غالبًا ما تتضمن تحسينات أمنية مهمة. يمكنك التحقق من وجود تحديثات من خلال إعدادات الجهاز، ويُنصح بتمكين خاصية "التحديثات التلقائية" لتبقى محميًا دون الحاجة للتحديث يدويًا. وإذا كنت تستخدم جهازًا قديمًا لم تعد الشركة المصنعة توفر له تحديثات، فعليك التفكير في استبداله بآخر يدعم التحديثات، حتى وإن لم يكن من الطراز الأحدث أو الأغلى، لأن التحديثات تبقى من أهم وسائل الحماية ضد الهجمات الإلكترونية. (https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/use-antivirus-software/ ،. 2025/05/03، 17:30)



الفصل الرابع:
الدراسة الميدانية

4. الدراسة الميدانية:

1.4. مرحلة ما قبل التصميم.

1 ـ المعلن:

جامعة المسيلة بولاية المسيلة.

2 ـ تحديد الموضوع

يتمحور موضوع حملتنا الإعلامية حول قضية باتت تُشكّل تحديًا أساسيًا في ظل التطور الإلكتروني المتسارع، وهي حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي .فقد أصبحت هذه الظاهرة تشغل حيزًا متزايدًا من اهتمام الأفراد والمجتمعات على حد سواء، لا سيما مع الانتشار الواسع لاستخدام المنصات الرقمية وتعدد أشكال التفاعل من خلالها.

نسعى من خلال هذه الحملة إلى تسليط الضوء على أهمية الوعي بخصوصية المستخدم، والتنبيه إلى ضرورة إعادة النظر في كيفية التعامل مع المعلومات الشخصية والبيانات الرقمية، التي باتت عرضة للاختراق أو الاستغلال في غياب الوعي الكافي. كما نهدف إلى تحفيز المجتمع على مراقبة هذا المجال المهم، وتبنّي سلوك رقمي مسؤول يواكب التطور الحاصل في وسائل الاتصال والتكنولوجيا الحديثة.

وتسعى الحملة أيضًا إلى تكثيف الجهود في مجال التوعية والتحسيس بالمخاطر التي قد تنجم عن إهمال حماية الخصوصية، سواء على المستوى الفردي أو الجماعي، لما لذلك من تأثيرات اجتماعية وأمنية ونفسية قد تكون خطيرة في بعض الحالات. إننا نؤمن أن تعزيز ثقافة الخصوصية هو جزء أساسي من الأمن الرقمي، ومسؤولية مشتركة بين الأفراد، والمؤسسات، والجهات التشريعية.

3 ـ تحديد الجمهور المستهدف:

تعد الخطوة الأولى في تنفيذ أي حملة إعلامية هي تحديد الجمهور الذي ستُوجه إليه الرسالة الإعلامية. وبناءً على طبيعة موضوع حملتنا، فقد اخترنا طلبة جامعة محمد بوضياف

بالمسيلة كجمهور مستهدف، نظرًا لكونهم من أكثر الفئات استخدامًا لشبكات التواصل الاجتماعي، وما يترتب عن ذلك من تحديات تتعلق بحماية الخصوصية، مما يستدعي توجيه الجهود التوعوية نحو هذه الفئة بشكل خاص.

4 ـ تحديد الأهداف:

موضوع حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي من القضايا الحيوية التي تكتسب أهمية متزايدة في ظل الانتشار الواسع للتكنولوجيا الحديثة .تتجلى هذه الأهمية بشكل خاص لدى الطلبة، الذين يُعتبرون من أكثر الفئات استخدامًا لهذه المنصات الرقمية .ورغم ذلك، يُلاحظ وجود محدودية في الوعي بثقافة حماية الخصوصية، ولهذا ركزت أهداف الحملة على:

5- نشر الوعي لدى الطلبة حول أهمية حماية الخصوصية على شبكات التواصل الاجتماعي.

6-التعريف بالمخاطر المرتبطة بكشف المعلومات الشخصية عبر المنصات الرقمية.

7-توجيه المستخدمين إلى كيفية ضبط إعدادات الخصوصية بطريقة فعالة وآمنة.

8-تعزيز الثقافة الرقمية المسؤولة لدى الشباب الجامعي.

9-الحد من الممارسات السلبية المرتبطة بالاستخدام العشوائي للمعلومات الشخصية.

10- خلق بيئة جامعية رقمية آمنة تحترم الخصوصية وتُعزز الاستخدام الواعي للتكنولوجيا.

5 ـ انتقاء الوسيلة الإعلامية:

الملصق: هو وسيلة بصرية فعّالة تُستخدم لنقل فكرة أو رسالة معينة من خلال مزيج من الصور والرسوم والكلمات. تُعد الملصقات أدوات اتصال جماهيري تُستخدم للتأثير على الجمهور وإقناعه، وتتنوع في أحجامها وأشكالها، تُستخدم الملصقات في مجالات متعددة، مثل الإعلان عن المنتجات، الترويج للأحداث، التوعية بالقضايا الاجتماعية، والتعليم. وتُعتبر الوسيلة الرئيسية في الحملة، حيث تهدف إلى جذب انتباه الجمهور وتوصيل الرسالة

بشكل مباشر وفعّال. في سياق حملتنا حول حماية الخصوصية على شبكات التواصل الاجتماعي، يُعتبر الملصق الإعلامي أداة مناسبة لمعالجة هذه الظاهرة، نظرًا لقدرتها على التأثير البصري وإيصال الرسائل التوعوية بشكل مبسط وجذاب.

2.4. مرحلة التصميم:

1 ـ طابع الرسالة:

على اعتبار أن موضوع حملتنا يدور حول حماية الخصوصية لمستخدمي شبكات التواصل الاجتماعي فإن أسلوب الحملة في هذه الحالة يكون أسلوب الإرشاد والنصح، حيث يحمل الكثير من الجدية حتى نتمكن من تحقيق ما نريد الوصول إليه، وبما أن الحملة موجهة إلى طلبة جامعة محمد بوضياف بالمسيلة، فإنه من غير المناسب أن تتسم بطابع فكاهي أو ترفيهي، إذ قد يُفقد ذلك الحملة قيمتها .لذا، يُعد أسلوب التخويف والنصح الأنسب لإيصال الرسالة إلى الجمهور، حيث يُسهم الخوف في إدراك الفرد لخطورة الموضوع، مما يدفعه للاهتمام بخصوصيته والنظر بجدية في أساليب حمايتها .وبهذا، يشعر الفرد بأن الأمر يعنيه شخصيًا، فكلما ازداد القلق، زاد الاهتمام بخصوصيته.

2 ـ نبرة الرسالة:

اتخذت رسالة الحملة الإعلامية التي قمنا بتصميمها طابعًا توعويًا يحمل نبرة إرشادية وناصحة، حيث ركزت على توجيه جميع طلبة جامعة محمد بوضياف بالمسيلة إلى ضرورة التحلي بالوعي الرقمي والمسؤولية الفردية أثناء استخدام منصات التواصل الاجتماعي. وجاءت الرسالة لتعزز الإدراك بأهمية حماية الخصوصية وعدم التهاون في مشاركة المعلومات والبيانات الشخصية،

3 ـ محتوى الرسالة: رسالتنا تركز على توعية مستخدمي شبكات التواصل الاجتماعي بأهمية حماية معلوماتهم الشخصية والرقمية وتعزيز مفهوم أن حماية الخصوصية مسؤولية فردية تبدأ من المستخدم نفسه.

4 ـ الملصق :حمل المضمون التالي:

في تصميم الملصق المعتمد للحملة الإعلامية، تم استخدام اللونين الأحمر والأزرق كخلفية رئيسية، حيث جاء اللون الأحمر في الجزء العلوي للدلالة على الخطر الذي قد ينجم عن عرض المعلومات الشخصية وانتهاك خصوصية مستخدمي شبكات التواصل الاجتماعي، وهو ما يعكس طبيعة التهديدات المحيطة بالمجال الرقمي. وقد تم وضع صورة قفل يُمسك به المستخدم أمام جهاز كمبيوتر، في إشارة رمزية إلى ضرورة التزام الأفراد بتطبيق آليات الحماية الرقمية، وتعزيز وعيهم بوجوب التحكم في إعدادات الخصوصية. كما تضمن الجزء العلوي أيضًا شعار جامعة محمد بوضياف باعتبارها الجهة الراعية والمشرفة على الحملة، ما يضفي عليها طابعًا رسميًا ويعزز مصداقيتها.

أما عنوان الحملة "حملة إعلامية لحماية خصوصية مستخدمي شبكات التواصل الاجتماعي"، فقد وُضع في منتصف الملصق بخط واضح وباللون الأسود، كونه الموضوع المحوري للحملة، وللدلالة على الجدية والسلطة في الطرح، بهدف جذب انتباه المتلقي وترسيخ أهمية الرسالة التوعوية.

في الجزء السفلي من الملصق، تم اعتماد خلفية باللون الأزرق لما يحمله هذا اللون من دلالات على الهدوء والثقة، وهي المشاعر المرجوة للمستخدم بعد تأمين بياناته وحماية خصوصيته. كما أن هذا اللون يرتبط برمزية "الفضاء الأزرق" التي تُطلق عادة على شبكات التواصل الاجتماعي نظراً لاعتماد أغلب تطبيقاتها هذا اللون في شعاراتها وواجهاتها.

وقد تم إدراج مجموعة من الرموز البصرية التي تعزز مضمون الحملة، مثل أيقونات أشهر منصات التواصل الاجتماعي (فيسبوك، إنستغرام، واتساب، ومنصة – X تويتر سابقًا)، إلى جانب صورة جهاز حاسوب وهاتف محمول في يد مستخدم يرمزان إلى الاستخدام الواعي والآمن بعد تفعيل أدوات حماية الخصوصية.

وأُختير شعار الحملة الإعلامية "شارك بحذر، وخلي خصوصيتك بأمان" ليكون في أسفل الملصق مكتوبًا باللون الأبيض، لما يحمله من بساطة ووضوح، حيث يلخص جوهر

الحملة ويوصل الرسالة الأساسية بفعالية، إلى جانب إدراج تاريخ انطلاق الحملة لتحديد الإطار الزمني لها.

5 ـ المطوية:

هي ورقة a4 تطو على ثلاثة بها معلومات حول موضوع الحملة " حماية خصوصية مستخدمي شبكات التواصل الاجتماعي، تعتبر الصفحة الأولى واجهة المطوية تحتوي على شعار جامعة محمد بوضياف وعنوان الحملة تحته شعار الحملة وبعض الصور في الخلفية التي تعبر عن الموضوع.

6 ـ توقيع الرسالة: توقيع الرسالة يعني علامة الخدمة المقدمة وتعكس واقع المؤسسة التي تدير الحملة ويعتبر هذا العنصر إحدى العناصر المهمة التي تضمن مصداقية الرسالة وتبعد عنها الشك أو الاشتباه حيث يحرص المصمم في نهاية إنجازه للتصميم على وضع توقيعه.

3.4. مرحلة ما بعد التصميم:

1 مدة الحملة: كلما طالت مدة الحملة كلما كان احتمال الحصول على نتائج إيجابية أكثر، أما عن المدة الزمنية التي تستغرقها الحملة فتبدأ من 05 ماي 2025 إلى 12 ماي 2025.

2 ـ تسلسل وقائع الحملة: أما عن تنفيذ حملتنا، ففضلنا أن تكون متواصلة لكي ترسخ الأفكار في ذهن الجمهور المستهدف بشكل أفضل وتعطي بعدا واسع للموضوع.

3 ـ أماكن تعليق الملصقات في الأماكن التالي:

-مدخل الجامعة، مساحة الجامعة، حافلات النقل الجامعي.

-**الميزانية** : تكلفة حملتنا تمثلت إجمالا في المبلغ الذي خصصناه لتصميم وطبع الملصق، قدر ثمن الملصق بـ1000 دج وثمن المطوية قدر 250 دج.

4 ـ التقييم : من خلال الملاحظة الميدانية، لوحظ تفاعل مقبول من طرف الطلبة مع محتوى الحملة، حيث أبدى العديد منهم اهتمامًا بالملصقات والمطويات المعروضة، ما يعكس وعيًا أوليًا بأهمية حماية الخصوصية.

خاتمة

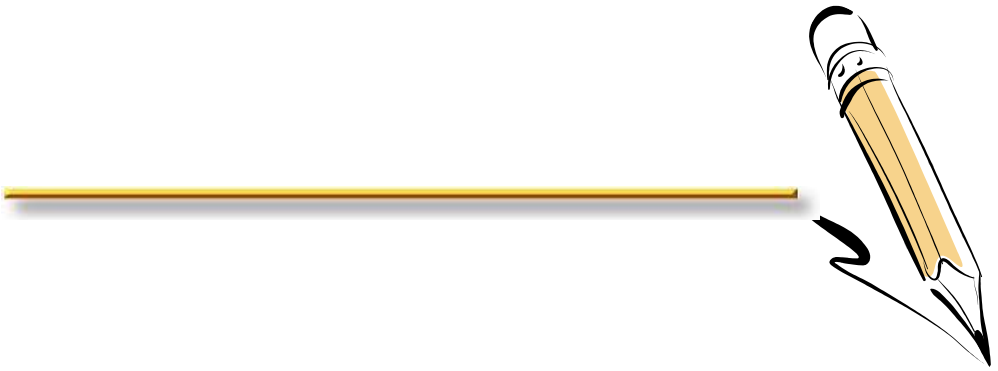
الخاتمة:

في عصر التحول الرقمي المتسارع، باتت شبكات التواصل الاجتماعي تشكل فضاءً افتراضياً يتيح للمستخدمين التعبير عن ذواتهم عبر هويات رقمية. غير أن هذه الحرية الظاهرة تخفي وراءها منظومة تحكم دقيقة تفرضها المنصات الرقمية، التي لا تكتفي بتحديد طبيعة التفاعل، بل تسهم في تشكيل العلاقات واقتراح المحتوى بما يخدم أهدافها التجارية.

ومع هذا الانخراط العميق، تتعرض خصوصية المستخدمين لتحديات خطيرة، أبرزها استغلال البيانات الشخصية في الإعلانات، أو حتى لأغراض أمنية، دون وعي أو موافقة صريحة من المستخدم. وهذا ما يستدعي وعياً رقمياً جديداً، يبدأ من إدراك الأفراد لمخاطر مشاركة البيانات، ويمر عبر تبني سلوك رقمي مسؤول، وتفعيل أدوات حماية الخصوصية.

وفي المقابل، يتحتم على الحكومات والمؤسسات المعنية التدخل من خلال سن تشريعات صارمة، وإلزام المنصات الرقمية باحترام خصوصية المستخدمين. كما يجب دمج مفاهيم الخصوصية والأمن الرقمي في التعليم، وتكثيف الحملات التوعوية، وتنظيم ندوات علمية وورش عمل لبناء وعي مجتمعي شامل حول هذه القضايا.

فالخصوصية الرقمية لم تعد شأناً فردياً، بل أصبحت مسألة مجتمعية وأمنية بامتياز، تتطلب تضافر الجهود التقنية، القانونية، والتربوية لضمان فضاء رقمي آمن وعادل للجميع.



قائمة المصادر والمراجع

قائمة المصادر والمراجع:

- ابن منظور الأنصاري الإفريقي المصري. (2003 م،ج 7).
- احمد عمي الدروبي. (2018، العدد 4). مواقع التواصل الاجتماعي وأثرها عمى العلاقات الاجتماعية. جامعة الكويت.
- أحمد مختار عمر. (1429). معجم اللغة العربية المعاصرة، الطبعة الأولى. القاهرة: عالم الكتب.
- أسامة عبد الله قايد، الحماية الجنائية لحق الانسان في صورته، مكتبة الألأء الحديثة،أسيوط بدون ط.
- أشرف جابر سيد. (2013 ص13). الجوانب القانونية لمواقع التواصل الاجتماعي، ومشكلات الخصوصية، . القاهرة: دار النهضة العربية.
- أمينة قراي. فعالية الحملات الإعلامية لمديرية الحماية المدنية في نشر الثقافة المرورية لدى تلاميذ الطور الثانوي، دراسة ميدانية على عينة من تلاميذ ثانوية فرحاتيا حميدة، أم بواقي، مذكرة لنيل شهادة الماستر في علوم الإعلام والاتصال، غير منشورة، كلية العلوم الإنسانية.
- بلعيد الدوكالي ، إبراهيم البوراصي. (2022). استباحة خصوصية بيانات المستخدم على الانترنيت ومدى وعي المستخدمين بها في ليبيا ، مجلة جامعة سبها للعلوم البحتة والتطبيقية، المجلد 21، العدد 2. ليبيا : جامعة طرابلس ليبيا .
- تباني، عبير. (2012). الحملات الإعلامية الإذاعية الخاصة بالتوعية المرورية في الجزائر .
- جمال الدين أبي الفضل محمد بن مكرم، لسان العرب، تحقيق عامر أحمد حيدر، مراجعة عبد المنعم خليل ابراهيم، دار الكتب العلمية، لبنان، ط 1، .
- حسام منصور. (2022). شبكات التواصل الاجتماعي، مدخل نضري لفهم الإيجابيات والسلبيات المؤتمر العلمي.

- حمدي محمد، إسماعيل. (2018). الحملات الإعلامية وفن مخاطبة الجمهور، دار المعتز للنشر والتوزيع، الطبعة الأولى، عمان.
- حنان أحمد سليم. " الحملات الإعلامية عبر الإعلام الجديد "، مجلة الرأي العام ، المجلد 12 ، العدد 01 ، يناير 2013.
- خالد زعموم. الديديولوجية وحملات التسويق الاجتماعي في الوطن العربي: كلية الاتصال، جامعة الشارقة، الامارات العربية، د.س.
- د. عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية عبر شبكات مواقع التوصل الاجتماعي، مصر: كلية الحقوق ، جامعة طنطا.
- د. غلاب صليحة وآخرون. (جوان 2017). فعالية الحملات الإعلامية في تنمية الثقافة المقاولاتية لدى الطالب الجامعي، دارسة ميدانية على عينة من طلبة جامعة 8 ماي 1945 قالمة، مجلة اقتصاديات المال والأعمال JFBE ، باتنة، الجزائر.
- د. مصطفى الناير المنزول. الحماية القانونية للحقوق الفنية والأدبية في السودان، مجلة الشريعة والقانون في جامعة إفريقيا العالمية – كلية الشريعة والقانون وكلية الدراسات الإسلامي.
- رزق سلمودي، ليندا ربايعة، هديل الرزي. (عام 2017) وعصام براهمة، الموقف المعاصر لقواعد القانون الدولي العام من الحق في الخصوصية في العصر الرقمي ،مجلة الجامعة العربية الأمريكية للبحوث، المجلد 3، العدد 2.
- سامح محمد عبد الحكيم. (2007). جرائم الانترنت الواقعة على الأشخاص في إطار التشريع البحريني، دراسة مقارنة بالتشريع المصري، ط 2، دار النهضة العربية، القاهرة.
- سمية أم لرقاب. (2020 – 2021). فعالية الحملات الإعلامية في مجال التوعية المرورية بالجزائر "دراسة ميدانية بالمركز الوطني للوقاية والأمن عبر الطرق"،

أطروحة مقدمة ضمن متطلبات نيل شهادة دكتوراه ل م د في شعبة علوم الإعلام والاتصال، تخصص إشهار وعلاقات عامة.

- الشاعر ، عبد الرحمان بن ابراهيم. (2015). مواقع التواصل الاجتماعي والسلوك الانساني. عمان ، الاردن: دار صفاء للنشر والتوزيع.
- الشوابكة ، محمد امين. (2007). جرائم الحاسوب والانترنيت – الجريمة المعلوماتية. عمان ، الاردن: دار الثقافة للنشر والتوزيع.
- صالح محمد الملك: حملات التوعية العامة والخطوات الأساسية اللازمة لنجاحها، ط 1، السبت 6 ربيع الثاني، العدد1. (1421).
- عابد زهير. (2014). الإعلام والبيئة بين النظرية والتطبيق، دار اليازوري للنشر و التوزيع ، مصر.
- عاطف يوسف. (سبتمبر – 2018). تخطيط الحملات الإعلامية، شعبة العلاقات العامة، جامعة المنوفية كلية الأدب.
- عبد الحي، محمد. (2012). مدخل تاريخي لنشأة وتطور التلفاز. أماباراك مجلة علمية محكمة تصدر عن الأكاديمية الأمريكية للعلوم والتكنولوجيا.المجلد الثالث.
- عصماني، سفيان. (2016). توظيف حملات التسويق الاجتماعي في التوعية لتعزيز مفهوم السلامة المرورية. مجلة العلوم الاقتصادية وعلوم التسيير. (العدد 16). كلية العلوم الاقتصادية والتجارية وعلوم التسيير.جامعة سطيف 1: الجزائر.
- الفراهيدي، الخليل بن أحمد،. (.سنة 1424 هـ 2003 م، ج 1). كتاب العين مرتبا على حروف المعجم، تحقيق عبد الحميد هنداوي، دار الكتب العلمية، لبنان ط1.
- محمد الزبيدي. تاج العروس من جواهر القاموس، ، الطبعة الثانية، ج 37.
- محمد سامي عبد الصادق. (2016). شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، القاهرة.

- محمد منصورى تأثير شبكات التواصل الإجتماعي على جمهور المتلقين، "الدنمارك: الأكادمية العربية المفتوحة، 2012 ".
- محمد نصر محمد. (2016). المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية (دراسة مقارنة) . مصر : مركز الدراسات العربية والتوزيع.
- محمد. (2008). حملات التوعوية المرورية، مركز الدارسات والبحوث ، المملكة العربية السعودية.
- المرسوم التشريعي رقم 01/94 ، المؤرخ في 15 جانفي 1994 ، المنشور في الجريدة الرسمية العدد 03 ، المؤرخة في 16 جانفي1994 ، السنة 31 المتعلقة بالمنظومة الاحصائية . . (بلا تاريخ).
- مصطفى الكافي. (2015). تخطيط الحملات الإعلامية والإعلانية MEDIA CAMPAIGN PLANNIG ، دار كمكتبة الحامد ، ط 1، عمان الأردن ، 1436.
- المعجم، تحقيق عبد الحميد هنداوي، دار الكتب العلمية، لبنان ط 1 .سنة 1424 هـ 2003 م، ج 1.
- ممدوح خليل بحر. (سنة 1403 هـ،. 1983 م). حماية الحياة الخاصة في القانون الجنائي، دراسة مقارنة، دار النهضة العربية، بدون ط.
- منصور القاضي، جيرار كورنو. (1418). معجم المصطلحات القانونية المؤسسة الجامعية للدراسات، هـ، الطبعة الأولى، . بيروت.
- مي كنعان. إدارة الحملات الإعلامية. عمان: دار أمجد للنشر والتوزيع، 2014.
- نسيمة، مقبل. محاضرات في مادة حملات الاتصال العمومي، مطبوعة دروس موجهة لطلبة السنة الثالثة ليسانس، السداسي الثالث تخصص اتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر 03 ، الجزائر. (2019 / 2020، ص 12).

- نى الاشقر جبور& محمود جبور. (2018). البيانات الشخصية والقوانين العربية: الهمّ الأمني وحقوق الأفراد، . بيروت – لبنان: المركز العربي للبحوث القانونية والقضائية مجلس وزراء العدل العرب، جامعة الدول العربية، الطبعة الأولى.

المواقع:

- https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/stay-safe-on-social-medi.(17:00 ،2025/05/03) .
- https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/use-antivirus-software /
- (17:30 ،2025/05/03)
- https://me.kaspersky.com/resource-center/preemptive-safety/how-to-protect-personal-online-privacy ،2025/05/03) . .(17:30
- https://me.kaspersky.com/resource-center/preemptive-safety/how-to-protect-personal-online-privacy ،2025/05/03) . .(17:30
- https://me.kaspersky.com/resource-center/threats/blackcat-ransomware.(22:40 ،2025/04/28 ،) .
- https://me.kaspersky.com/resource-center/threats/hackers-and-email-addresses.(23:20 ،2025/04/28) .
- https://me.kaspersky.com/resource-center/threats/sim-swapping.(22:50 ،2025/04/28) . ،

- https://me.kaspersky.com/resource-center/threats/vidar-stealer .(.22:25 ،2025/04/28) .
- https://stopthinkfraud.campaign.gov.uk/how-to-spot-fraud/how-to-spot-postal-fraud.(17:00 ،2025/05/03) ./
- https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/stay-safe-on-social-media.(.17:00 ،2025/05/03) . /
- Maria Pirzada, sample privacy policy template, https://www.privacypolicies.com/blog/privacy-policy-template,(consulté le 25/08/2226،(l04l2025.(بلا تاريخ) .18:55،
- http://www.namaa.com sa/ le 25/03/2019-18:55.
- https://www.terranovasecurity.com/blog/data-privacy-social-media-protect-your-information.(45 :18 ,2025/04/30) .

الملاحق

الملاحق

الملحق رقم (1): ملصق

الملحق رقم (2): الوجه الأول

"خصوصيتك غالية ... لا تهملها في ضغطة زر!"

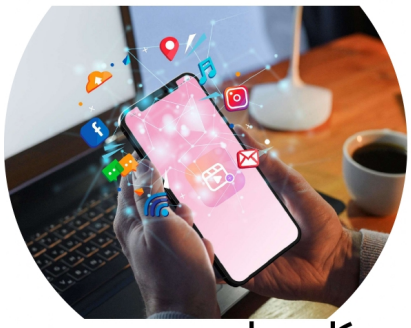
8 ـ افحص جهازك دورياً للتأكد من خلوه من الفيروسات وبرامج التجسس المعروفة ب (Spyware) وبرامج الدعاية المعروفة بـ (ad-ware) فهذه البرامج تتبع نشاطاتك واهتماماتك (من خلال المواقع التي تقوم بزيارتها), ثم ترسل معلوماتك التي تجمعها إلى المنظمات والشركات التي أنتجتها.

9 ـ كذلك قم بتحديث نظام التشغيل والمتصفح بشكل منتظم من خلال مواقع الشركات المنتجة لها (لسد الثغرات التي قد يتسلل منها المخترقونلسرقةالملفات والمعلومات الشخصية.

10ـ استخدم التشفير لحماية ملفاتك الإلكترونية التي تحتوي على معلومات شخصية هامة.

11 ـ قد تكون ملفات كوكيز (وهي ملفات نصية تحفظ في جهاز المستخدم أثناء زيارة بعض المواقع) تهديدًا لخصوصيتك ,

لذا عليك التخلص من ملفات الكوكيز غير الضرورية من فترةلأخرى وذلك عن طريق الخيارات التي توجد في متصفح الإنترنت.



كل حساب محمي ... يعني شخص مرتاح.

الملحق رقم (3): الوجه الثاني

خطوات حماية الخصوصية على مواقع التواصل اجتماعي

1ـ يجب عدم إعطاء المعلومات الشخصية لمواقع الإنترنت إلا عند الضرورة, ويجب التأكد من هوية الموقع وأنه يمثل منشأة معروفة, وعلى المستخدم الاطلاع الدقيق على سياسة حماية الخصوصية التي يتبعها الموقع للتأكد من عدم احتوائها على شروط قد تخل بالخصوصية وتسمح للموقع بالتصرف بالمعلومات, فالكثير من المستخدمين يوافقون على الشروط دون الاطلاع عليها, وعلى الجانب الآخر تجنب المغامرة بإعطاء معلوماتك للمواقع غيرالموثوقة مثل المنتديات وغيرها.

2ـ إن التعامل مع أشخاص مجهولي الهوية من خلال شبكة الإنترنت يحتم توخي الحذر وعدم المجازفة بإعطاء معلومات تخص المستخدم, وكذلك عدم إبداء الثقة مباشرة مع أي شخص أو موقع على الشبكة , فبرامج المحادثة والمنتديات ومشاركة الملفات كلها أدوات يجب استخدامها بحذر, كما ينبغي تنبيه الأطفال وتعليمهم أهمية حماية خصوصياتهم وخصوصيات أسرهم, وعدم تسريب المعلومات الشخصية للغرباء على شبكة الإنترنت, واستشارة الوالدين عند مواجهتهم لمثل هذه المواقف.

3ـ لا تستخدم أجهزة الحاسبات العامة مثل مقاهي الإنترنت أومعامل الجامعة للوصول إلى معلوماتك الشخصية الهامة, فقد تكون عرضة للمراقبة من خلال برامج التجسس أو المخترقين.

"شارك بحذر ،وخلي خصوصيتك بأمان"

4 ـ ضرورة تصميم سياسات الخصوصية في المنشآت لحماية المعلومات الشخصية للموظفين والعملاء , وهذا أمر أساسي في سبيل حماية المعلومات الشخصية من الاستخدام غير نص تكميلي قصير المشروع, فالسياسات والإجراءات يجب أن تحدد كيفية تخزين المعلومات والدخول إليها وتنظيمها وحمايتها وذلك باستخدام تقنية التشفير, وتنظيم الدخول والتدقيق في سجلات الدخول للمعلومات لاكتشاف أي عمليات غير مشروعة وإيقافها ومحاسبة المتسببين في ذلك, كما يجب عدم إفشاء المعلومات لطرف ثالث دون الرجوع لصاحب هذه المعلومات وأخذ الإذن منه لتجنب أي ملاحقة قانونية.

5 ـ تقوم بعض المواقع على شبكة الإنترنت بجمع معلومات شخصية عن المستخدم قد تساعد في تحديد هويته واهتماماته, فعلى سبيل المثال تقوم مواقع البحث الشهيرة باستخدام البريد الإلكتروني الذي تقدمه هذه المواقع لتحديد هوية المستخدم والكلمات والمواضيع التي يبحث عنها, بل إن بعض المواقع مثل ياهو (yahoo) صرّح بأنه يقوم بجمع معلومات شخصية لأصحاب البريد.

6 ـ لا تعتمد رقماً سرياً موحدًا لجميع حساباتك على الإنترنت, ولكن استخدم كلمات سر مختلفة بحسب أهمية الحساب, مع ضرورة تجنب استخدام كلمات سر سهلة التخمين .

7 ـ يفضل عدم إرسال معلومات شخصية إلا من خلال قناة مشفرة باستخدام بروتوكول (https), لأن بروتوكول التشفير
يعتمد على شهادة إلكترونية تصدر من جهة مستقلة تتحقق من هوية الموقع قبل إصدارها, وتنتقل البيانات داخل قناة مشفرة بحيث لا يستطيع أحد الاطلاع عليها أثناء انتقالها, وللتعرف على نوع البروتوكول يمكن للمستخدم قراءة حقل العنوان في المتصفح والتأكد من أنه يبدأ بحروف (https) , أو
التأكد من وجود علامة القفل في إحدى زوايا المتصفح.

لاتمنح العالم مفاتيح حياتك خصوصيتك درعك

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
جامعة محمد بوضياف بالمسيلة
University Mohamed Boudiaf of M'sila
1985
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila
كلية العلوم الإنسانية والاجتماعية
FACULTY OF HUMANITIES AND SOCIAL SCIENCES
Faculty of Humanities and Social Sciences
Vice-Deanship of the College for Studies and Student Issues
كلية العلوم الإنسانية والاجتماعية
نيابة العمادة للدراسات والمسائل المرتبطة بالطلبة
قسم علوم الاعلام والاتصال

الرقم: /٢٩٩

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية لإنجاز بحث

انا الممضي (ة) ادناه : السيد(ة): مختاري فيصل

الصفة(طالب، استاذ باحث، باحث دائم): طالب

الحامل لبطاقة التعريف الوطنية رقم: 203511804

الصادرة بتاريخ : 2018/10/09 عن دائرة : أولاد جلال

المسجل(ة)بكلية: العلوم الانسانية والاجتماعية قسم: علوم الاعلام والاتصال

تخصص: اتصال وعلاقات عامة تحت رقم التسجيل: 200750167 08

والمكلف بإنجاز اعمال بحث(مذكرة التخرج، مذكرة ماستر ' مذكرة ماجستير ' اطروحة دكتوراه) .

عنوانها: تصميم حملة إعلامية لحماية خصوصية مستخدمي مواقع التواصل الاجتماعي

اصرح بشرفي بانني التزم بالمعايير العلمية والمنهجية ومعايير الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور اعلاه

المسيلة في: 2025/06/01

امضاء المعني(ة):

شهد على المصادقة على الإمضاء
السيد: ...
بتاريخ: 3 جوان 2025

المرجع: القرار الوزاري رقم: 933 المؤرخ في: 28-07-2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها.

الجمهورية الجزائرية الديمقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
جامعة محمد بوضياف بالمسيلة
University Mohamed Boudiaf of M'sila
Faculty of Humanities and Social Sciences
Vice-Deanship of the College for Studies and Student Issues

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila
كلية العلوم الإنسانية والاجتماعية
نيابة العمادة للدراسات والمسائل المرتبطة بالطلبة
قسم علوم الاعلام والاتصال

وثيقة ايداع المذكرة

الموضوع: تصميم حملة إعلامية لجباية الموطنين مستخدما تكنولوجيا التواصل الاجتماعي.

إعداد الطالب :

1- مختاري ضحى رقم التسجيل: 2007S106708

القسم: علوم الاعلام والاتصال **الشعبة:** علوم الاعلام والاتصال تخصص: اتصال وعلاقات عامة

إشراف: ..... **الرتبة:** أستاذ

أقر بأنني تابعت العمل المذكور أعلاه في جلسات إشرافية طيلة الموسم الجامعي: 2024-2025 وأسمح بإيداعه على مستوى ادارة القسم للمناقشة والتقييم.

موافقة وإمضاء الاستاذ(ة) المشرف(ة):

رئيس فريق الاختصاص

رئيس القسم

رئيس قسم علوم الإعلام والإتصال
يوسفي عبد العالي

الملخص

ملخص

تتناول هذه المذكرة موضوع حماية الخصوصية الرقمية لمستخدمي شبكات التواصل الاجتماعي، في ظل التزايد الكبير لحالات انتهاك البيانات الشخصية والمعلومات الحساسة عبر هذه المنصات. وتركز على أهمية التوعية الإعلامية كوسيلة فعّالة لنشر ثقافة الحماية الرقمية، من خلال تصميم حملة إعلامية توعوية تساهم في تعزيز الوعي المجتمعي بمخاطر الاستخدام غير الآمن، وتشجع على اتباع سلوكيات تحافظ على خصوصية الأفراد أثناء تفاعلهم عبر الإنترنت.

الكلمات المفتاحية:

الخصوصية الرقمية – شبكات التواصل الاجتماعي – الانتهاكات الإلكترونية – الحماية المعلوماتية – التوعية الإعلامية – الحملة الإعلامية – أمن المعلومات – السلوك الرقمي.

Abstract:

This memo addresses the issue of digital privacy protection for social media users, amid the increasing number of cases involving the violation of personal data and sensitive information on these platforms. It highlights the importance of media awareness as an effective tool to promote a culture of digital protection, through the design of an awareness campaign that aims to raise public consciousness about the risks of unsafe online behavior and encourage practices that help safeguard users' privacy while interacting on the internet.

Keywords:

Digital privacy – Social media networks – Cyber violations – Information protection – Media awareness – Media campaign – Information security – Digital behavior