دراســـات

الخصوصية والأمن السيبراني في المجتمع السعودي..

أهمية المسؤولية في ممارسة الحرية الرقمية

مركز القرار
للدراسات الإعلامية

يناير
2022

الرسالة:

رفد المجال الإعلامي بالبحوث والدراسات المنهجية التأصيلية، وتقويم أداء وسائل الإعلام التفاعلي، ورصد وتحليل مضامينها.

من نحن:

مركز سعودي (مستقلّ)..

مضامين وسائل الإعلام التفاعلي .. ميداننا

بياناتها ووسائط محتواها .. حقول دراساتنا

الرصد والتحليل والقياس .. أدواتنا

أهدافنا:

- قياس اتجاهات الرأي العام وتأثيراتها
- تقويم الخطاب الإعلامي، والارتقاء به
- رصد تحوّلات ثورة الاتصالات والمعلومات
- تقديم التوصيات المنهجية
- استشراف المستقبل.. وفق قواعد البحث العلمي

المحتويات

ملخص تنفيذي..

تُعد التهديدات السيبرانية من أخطر وأعقد التهديدات التي تستهدف الدول والأفراد على حدٍّ سواء، نظرًا لطبيعتها المتطورة وتكلفتها الضئيلة، الأمر الذي يكشف أهمية دور الأمن السيبراني المعني بحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تستهدف عادة الوصول للمعلومات السرية أو إتلافها، أو ابتزاز المستخدمين وانتهاك خصوصياتهم وأمن معلوماتهم الشخصية، وغيرها من سلوكيات تضر المستهدفين.

وتجدر الإشارة إلى وجود علاقة طردية بين أهمية الأمن السيبراني واستخدام التكنولوجيا، حيث تزداد هذه الأهمية كلما ارتفع حجم الاعتماد على التقنيات الحديثة.

وبالنظر إلى السياسة التي تتبعها الدولة السعودية منذ انطلاق رؤية المملكة 2030، وخاصة في شقها المتعلق بالتحول الرقمي وتنمية البنية التحتية الرقمية، تبرز أهمية وضرورة تعزيز منظومة الأمن السيبراني ووضعها ضمن أولويات المملكة، وهو ما تم بالفعل، وكان من مظاهره تأسيس الهيئة الوطنية للأمن السيبراني والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم 6801 بتاريخ 1439/2/11هـ، لتُصبح الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه ودعمه وتعزيزه.

ومن أجل استكشاف مدى إدراك المجتمع لأهمية الخصوصية والأمن السيبراني، والتعرف على دور كل من الدولة ووسائل الإعلام في عملية التثقيف والتوعية المجتمعية بهذا المجال الحيوي، قام مركز القرار للدراسات الإعلامية بدراسة قضية الخصوصية والأمن السيبراني، وذلك عبر ثلاثة مستويات من التحليل:

- الأول: تحليل خطاب مقالات كُتّاب الرأي التي تناولت قضية الخصوصية والأمن السيبراني في الصحف السعودية، وذلك بهدف التعرف على طبيعة ومضمون الرسائل الاتصالية التي قدموها في هذا الصدد.
- الثاني: تحليل مضمون حساب «الهيئة الوطنية للأمن السيبراني» على تويتر، بهدف التعرف على طبيعة الرسائل الاتصالية التي تُقدمها المؤسسات والهيئات الحكومية المعنية بالأمن السيبراني.
- الثالث: تحليل طبيعة تفاعلات المستخدمين السعوديين حول قضية الخصوصية المعلوماتية، واستكشاف مدى إدراكهم لأهمية الأمن السيبراني.

مقدمة..

أتاحت التطورات السريعة والمتلاحقة في مجال تكنولوجيا المعلومات والاتصالات كمًّا هائلاً من البيانات التي أصبحت بمثابة ثروة معلوماتية أحدثت تحولًا في مفهوم المعلومات من جانبين، الأول يتمثل في اختلاط العام بالخاص، أما الثاني فيتعلق بأنه في العصر الرقمي أصبح لـ «البيانات الضخمة- Big Data» أهمية كبيرة جعلت العديد من الجهات تتهافت للحصول عليها بشتى الطرق التي قد تتجاوز أحيانًا أخلاقيات الخصوصية؛ الأمر الذي يُبرز أهمية التخطيط الجيد لمواجهة هذه الفوضى بدلاً من انتظار آثارها التي بدت جلية بظهور عصابات الإنترنت، وتنامي معدلات الجرائم الإلكترونية والتهديدات السيبرانية بنسب فاقت المتوقع.

وتُعد التهديدات السيبرانية من أخطر وأعقد التهديدات التي تستهدف الدول والأفراد على حدٍّ سواء، نظرًا لطبيعتها المتطورة وتكلفتها الضئيلة، الأمر الذي يكشف أهمية دور الأمن السيبراني المعني بحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تستهدف عادة الوصول للمعلومات السرية أو إتلافها أو ابتزاز المستخدمين، وانتهاك خصوصياتهم وأمن معلوماتهم الشخصية، وغيرها من سلوكيات تضر المستهدفين.

وقد ارتبط بهذه التطورات بروز مجموعة من المصطلحات منها على سبيل المثال لا الحصر:

الخصوصية المعلوماتية: ويُقصد بها حق المستخدم في التحكم بالمعلومات الخاصة به، عبر مجموعة من القواعد التي تحكم عمليات جمع وإدارة وتحميل البيانات الخاصة، بهدف حمايتها من مختلف جرائم المعلوماتية؛ كالاختراق والاستغلال.

أمن المعلومات: ويعني العمل على توفير نظام لحماية وتأمين البيانات والمعلومات المتداولة ضد محاولات اختراقها واستغلالها.

البيانات الضخمة: عبارة عن مجموعة كبيرة من البيانات يتم جمعها وتخزينها والتعامل معها باستخدام أدوات تكنولوجية حديثة بهدف ترتيبها وتنظيمها وإدارتها وتحليلها بشكل يُناسب احتياجات المستفيدين.

وعلى الرغم من أهمية البيانات الضخمة والفوائد المتحققة من جمعها وتحليلها، فإن التهافت عليها صاحبه تحديات أمنية ترتبط بالخصوصية وأمن المعلومات التي يتم انتهاكها أحيانًا بالاستخدام والاستغلال غير المشروع لها من خلال ارتكاب العديد من التجاوزات، بدءًا من التجسس والسرقة والابتزاز والتطفل على الحياة الخاصة، وصولًا إلى تهديد الأمن القومي للدول.

هذه التحديات تستوجب ضرورة الاهتمام بالأمن السيبراني، وتثقيف المجتمع بمخاطر الإنترنت، والعمل على زيادة الوعي بأهمية الحفاظ على الخصوصية، والتعريف بالمصادر التي تُشكل تهديدًا لأمن المعلومات، وذلك من أجل الاستعداد لمواجهة أي هجمات خبيثة أو وسائل احتيالية لسرقة البيانات، والنجاح في التصدي لها.

وتجدر الإشارة هنا إلى وجود علاقة طردية بين أهمية الأمن السيبراني واستخدام التكنولوجيا، حيث تزداد هذه الأهمية كلما ارتفع حجم الاعتماد على التقنيات الحديثة.

وبالنظر إلى السياسة التي تتبعها الدولة السعودية منذ انطلاق رؤية المملكة 2030 وخاصة في شقها المتعلق بالتحول الرقمي وتنمية البنية التحتية الرقمية، تبرز أهمية وضرورة تعزيز منظومة الأمن السيبراني ووضعها ضمن أولويات المملكة، وهو ما تم بالفعل، وكان من مظاهره تأسيس الهيئة الوطنية للأمن السيبراني، والموافقة على تنظيمها بموجب الأمر الملكي الكريم رقم 6801 بتاريخ 1439/2/11هـ، لتُصبح الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه ودعمه وتعزيزه.

وخلال فترة قياسية، حققت السعودية نجاحًا وتميزًا نوعيًّا في هذا المجال الحيوي بفضل الله – عزّ وجل - ثم بفضل سياسات وتوجيهات القيادة الرشيدة – حفظها الله – فاحتلت المملكة المرتبة الثانية في المؤشر العالمي للأمن السيبراني الصادر عن وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات؛ الأمر الذي يعكس مدى حرص الدولة والقيادة الرشيدة على توفير فضاء سيبراني آمن للأفراد والمؤسسات، وبما يُمكّن من توفير بيئة خصبة للنمو والازدهار في كافة المجالات.

انطلاقًا مما سبق، سعى مركز القرار للدراسات الإعلامية لاستكشاف مدى إدراك المجتمع لأهمية الخصوصية والأمن السيبراني، والتعرف على دور كل من الدولة ووسائل الإعلام في عملية التثقيف والتوعية المجتمعية بهذا المجال الحيوي.

ومن أجل تحقيق ذلك، فقد اعتمدت الدراسة على ثلاثة مستويات من التحليل:

الأول: تحليل خطاب مقالات كُتّاب الرأي التي تناولت قضية الخصوصية والأمن السيبراني في الصحف السعودية، وذلك بهدف التعرف على طبيعة ومضمون الرسائل الاتصالية التي قدموها في هذا الصدد.

الثاني: تحليل مضمون حساب «الهيئة الوطنية للأمن السيبراني» على تويتر، بهدف التعرف على طبيعة الرسائل الاتصالية التي تُقدمها المؤسسات والهيئات الحكومية المعنية بالأمن السيبراني.

الثالث: تحليل طبيعة تفاعلات المستخدمين السعوديين حول قضية الخصوصية المعلوماتية، واستكشاف مدى إدراكهم لأهمية الأمن السيبراني.

أولًا

تحليل خطاب مقالات كُتّاب الرأي في الصحف

اعتمدت الدراسة على عينة عمدية مكونة من (56) مقالة تناولت قضية الخصوصية والأمن السيبراني، تم نشرها في الصحف السعودية مثل (الرياض، عكاظ، الوطن، المدينة، الشرق الأوسط) خلال الفترة من يناير 2020 وحتى أغسطس 2021م.

واعتبرت الدراسة أن المقال هو الوحدة الموضوعية للتحليل، وبناءً على ذلك فقد انتهت النتائج إلى ما يلي:

الأطروحات المركزية

قدّم كُتّاب الرأي في الصحف السعودية خلال تناولهم قضية الخصوصية والأمن السيبراني مجموعة من الأطروحات المركزية المُعَزِّزة بعدد من الحُجج والبراهين لإثبات صحة كل طرح، فجاء تناولهم متنوعًا شمل جهود المملكة العربية السعودية في مجال الأمن السيبراني، ومدى وعي المواطنين بأهمية الحفاظ على خصوصية بياناتهم الشخصية، والمخاطر التي قد تنتج عن اختراق خصوصية الأفراد والمؤسسات والدول، إضافة إلى تسليع البيانات الشخصية للأفراد بشكل انتهازي.

وتمثلت أهم الأطروحات المركزية فيما يلي:

1. تميز المملكة في مجال تحقيق الأمن السيبراني ومنع اختراق مؤسساتها

حيث تناول الكُتّاب اهتمام المملكة بالأمن السيبراني، وجهودها في هذا الصدد، التي جعلتها تتبوأ مكانة متقدمة على المستوى العالمي، وقد استشهدوا بالعديد من الحُجج المبرهنة على ذلك، ومنها:

- القفزة التكنولوجية التي حققتها المملكة منذ إطلاق رؤية 2030 في تحقيق الأمن السيبراني.
- حصول المملكة على المرتبة الثانية عالميًّا من بين 193 دولة، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني عام 2021 والصادر عن وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات «الاتحاد الدولي للاتصالات».

- إطلاق المنتدى الدولي للأمن السيبراني بالرياض لتوطين التجارب العالمية في عموم مكونات الأمن السيبراني، والذي يعد من أكبر المنتديات المعنية بهذا المجال.
- إطلاق صاحب السمو الملكي الأمير محمد بن سلمان ولي العهد – حفظه الله - مبادرتين دوليتين لتعزيز حماية الفضاء السيبراني، الأولى مبادرته الدولية لحماية الأطفال في الفضاء السيبراني، والثانية مبادرته لتمكين المرأة في الأمن السيبراني.
- تأسيس الهيئة الوطنية للأمن السيبراني في عام 2017 للتأكيد على أهمية الدور المأمول لحماية مؤسسات المملكة من أي هجمات إلكترونية خبيثة.

2. عدم إدراك بعض المستخدمين لأهمية حماية البيانات الشخصية

وفي هذا الطرح استعرض الكُتّاب نماذج من التعاملات المستهترة بأمن وخصوصية البيانات، ومنها:

- تراجع أهمية الخصوصية أمام الرغبة في تحقيق الشهرة والمكسب المادي.
- التهافت على إنشاء الحسابات في المنصات الاجتماعية المختلفة مع غياب الجانب الرقابي للأسرة.
- قيام العديد من المستخدمين بالموافقة على شروط وبنود الخصوصية في التطبيقات والمواقع دون الاطلاع عليها وقراءتها.
- عدم الإدراك بأن كل خطوة نخطوها تُوفر معلومات شخصية يتم تدوينها وتصنيفها، ومن ثمّ يتم تتبعنا عبرها في العالم الافتراضي.
- أكد الكُتّاب على أهمية تحصين أفراد المجتمع فكريًّا من سوء توظيف منصات التواصل الاجتماعي والتطبيقات الذكية، والتوعية بدور الأمن الإلكتروني في حماية البيانات والمعلومات الشخصية، مشددين على أن انتهاك خصوصية المستخدمين هي من سلبيات مواقع التواصل الاجتماعي.

3. الأمن السيبراني يُهدد الأمن القومي للدول

سعى كُتّاب الرأي في هذا الطرح إلى إبراز خطورة انتهاك الخصوصية، التي تتخطى حدود التأثير على الأفراد لتصل إلى تهديد المجتمعات والأمن القومي للدول، ومن استشهاداتهم على ذلك:

- الفضاء السيبراني لا يزال يعمل وفق منهج عدم الإفصاح بين الدول، فلا يوجد تعاون في وقف الهجمات والاختراقات السيبرانية.

- الهجوم السيبراني هو الصراع المستقبلي بين الدول، والحروب القادمة هي حروب تكنولوجية في المقام الأول؛ الأمر الذي يستوجب معه ضرورة تعزيز الأمن السيبراني لحماية الدول من الاستهداف.
- أضحت التدخلات السيبرانية تستخدم لتحقيق أهداف سياسية عدة، منها توجيه مواطني الدول الأخرى خلال العمليات الانتخابية في بلدانهم.
- قيام شركات وسائل التواصل الاجتماعي باختراق خصوصية الأفراد والحصول على معلومات تُستغل لمعرفة الوضع العام للمواطنين في دولهم.
- تستهدف الهجمات السيبرانية أيضًا المؤسسات التجارية والصناعية الحكومية، لاختراق خصوصياتها والحصول على بياناتها واستغلالها في عمليات الابتزاز المالي أو السياسي، أو تدمير هذه البيانات للإضرار باقتصاد الدولة.
- الساحة الإلكترونية أصبحت ساحة المعركة الرئيسية بين الغرب والشرق.
- الصراع السيبراني سيكون له تأثير كبير على السلامة العامة وصناعة النفط والغاز في العالم.
- قامت الولايات المتحدة الأمريكية بحظر التعامل مع الشركات المالكة لبعض التطبيقات التي ترى أنها تمثل تهديدًا لأمنها القومي.
- ساق الكُتّاب أمثلة للاعتداءات السيبرانية بين الدول، كمسؤولية إيران عن النشاط السيبراني التخريبي في المنطقة العربية، ومنها هجماتها التي حاولت بواسطتها اختراق المؤسسات السعودية خاصة شركة أرامكو التي نجحت في التصدي لها. وأيضًا تعرض الولايات المتحدة الأمريكية لسلسلة من الهجمات السيبرانية كتلك التي استهدفت وزارتي الخزانة والتجارة.

4. «تسليع» بيانات المستخدمين

سلّطت بعض مقالات الرأي في الصحف السعودية الضوء على استغلال مواقع التواصل الاجتماعي للبيانات الخاصة بالمستخدمين بهدف تحقيق مكاسب مادية، وذلك من خلال استخدامها كسلعة يتم بيعها للعلامات التجارية.

وعرض الكُتّاب مجموعة من الاستشهادات المبرهنة على ذلك، ومنها:

- استحواذ مواقع التواصل الاجتماعي على سوق الإعلانات العالمية بفضل البيانات والمعلومات المتوفرة لديها عن المستخدمين، بعدما كانت هذه السوق في السابق تحت سيطرة وسائل الإعلام التقليدية المرئية والمسموعة والمقروءة.
- مُطالبة حكومات بعض الدول شركات المنصات الاجتماعية بضرورة دفع أموال كضريبة على المكاسب التي تتحصل عليها الأخيرة من مواطني هذه الدول نتيجة استخدامهم للمنصات.

- قيام شركات وسائل التواصل الاجتماعي باختراق خصوصية الأفراد والحصول على معلومات يتم بيعها للعلامات التجارية التي تقوم بترتيبها وتحليلها، ومن ثمّ استخدامها بشكل تجاري لتحقيق مكاسب مادية.
- يتم اختراق خصوصية الأفراد والمؤسسات بالموافقة على شروط «واتساب» الجديدة، والذي يقوم بدوره بإتاحة المعلومات الخاصة بالمستخدمين لمنصة فيسبوك.
- أصبحت حماية خصوصية الأفراد واحدة من أهم المميزات التنافسية التي تلجأ إليها شركات الهواتف المحمولة ومواقع التواصل الاجتماعي من أجل كسب الجمهور.
- تتبادل نحو 90% من التطبيقات المجانية على متجر «جوجل بلاي» بيانات المستخدمين مع شركة «ألفابت» وهي الشركة الأم لجوجل، وتستخدم تلك البيانات في العديد من الأغراض التسويقية أو الدراسات والبحوث.

المعالجة الموضوعية للتهديدات السيبرانية

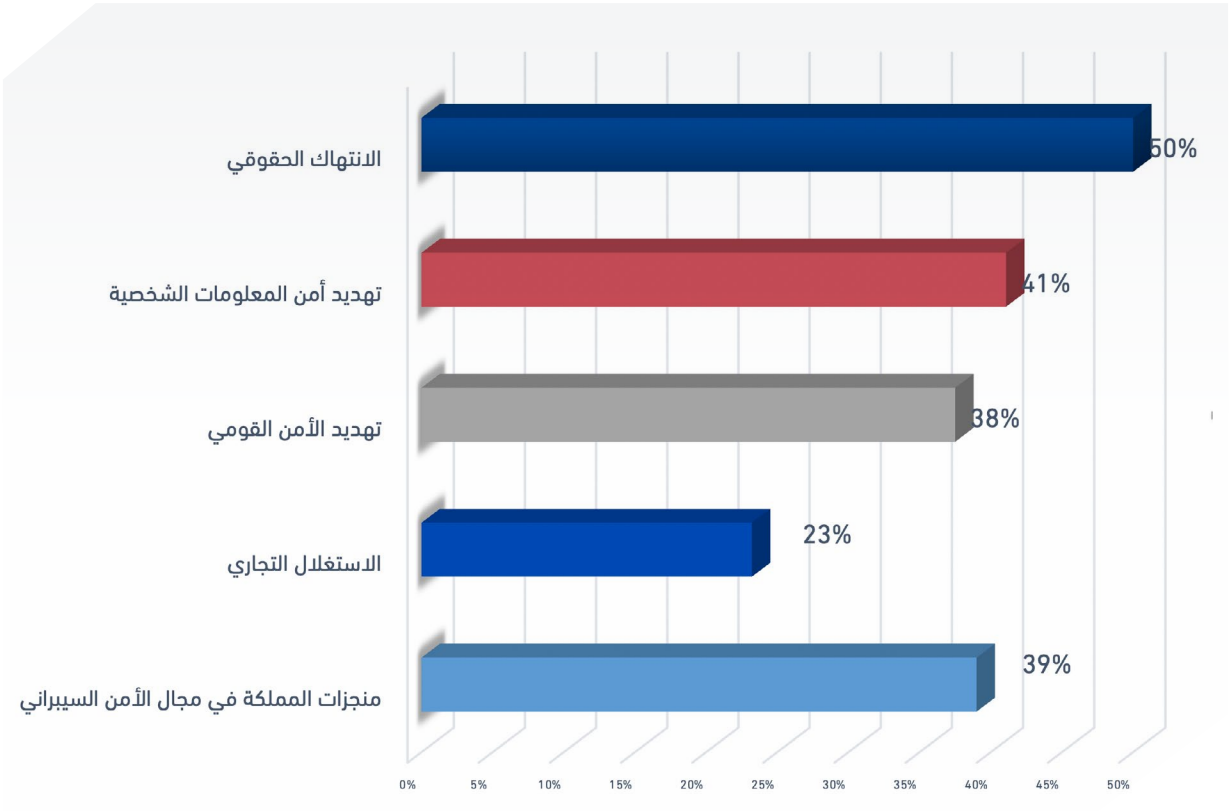
أوضحت النتائج أن معالجة كُتّاب الرأي لقضية التهديدات السيبرانية وخطورتها على خصوصية وأمن المعلومات اعتمدت على إبراز مجموعة من التهديدات جاء في مقدمتها «الانتهاك الحقوقي» لخصوصية المستخدمين، وفيها ركّز الكُتّاب على قيام شركات التواصل الاجتماعي بانتهاك حقوق المستخدمين، واستشهدوا بشروط «واتساب» الأخيرة التي كانت مثار الكثير من الجدل حول العالم بسبب إتاحتها إمكانية تبادل بيانات المستخدمين مع مواقع أخرى كـ «فيسبوك»، وبشكل يسمح للشركات الإعلانية والتجارية الحصول على هذه البيانات الشخصية، على أن يتم حذف الحسابات الرافضة للشروط؛ وبالتالي تمحور هذا التهديد حول السلوك غير الشرعي من جانب الشركات التكنولوجية.

أما فيما يخص «تهديد أمن المعلومات الشخصية» للأفراد، فقد ركّز كُتّاب الرأي تناولهم على السلوكيات غير المسؤولة من قِبل المستخدمين والتي تُسهل عملية اختراق حساباتهم والحصول على معلوماتهم وبياناتهم الخاصة دون إذن مسبق، ومن هذه النماذج هؤلاء الأشخاص الذين يمتلكون رغبة وإصرارًا على التواصل والظهور عبر مواقع التواصل الاجتماعي لتحقيق الشهرة والانتشار، وفي سبيلهم لتحقيق ذلك يتراجع حرصهم على خصوصية بياناتهم. كما يدخل ضمن هذه الفئة أيضًا المستخدمون الذين يجهلون بنود الخصوصية، ويُسارعون بالموافقة عليها دون تحقق أو مراجعة لها.

وتطرّق كُتّاب الرأي أيضاً في مقالاتهم إلى التهديدات التي تواجه الدول نتيجة اختراق خصوصية البيانات، ففي هذه الحالة يتم استهداف بيانات الشركات والمؤسسات الحكومية لا سيما الاقتصادية، واستعرض الكُتّاب التأثيرات السلبية المترتبة على ذلك الاختراق، التي قد تُهدد استقرار الدول، وتساهم في زعزعة أمنها القومي. إذ أكد بعضهم أن الحروب الإلكترونية أصبحت أشد فتكًا من الحروب التقليدية.

وتضمنت مقالات الرأي في الصحف السعودية أيضًا نوعًا آخر من التهديدات يتعلق بـ «الاستغلال التجاري» لخصوصية المستخدمين، حيث تلهث الشركات التكنولوجية وراء بياناتهم الشخصية التي أصبحت بمثابة سلعة ثمينة يمكن استخدامها لتحقيق مكاسب مادية وغير مادية، كالتأثير والتضليل وما إلى ذلك. وأوضح كُتّاب الرأي أنه باتت هناك شركات تشبه «سماسرة البيانات» تقوم ببيع معلوماتنا الخاصة كاهتماماتنا وعمليات البحث التي نقوم بها والمنتجات التي نُفضل الاطلاع عليها، وحتى توجهاتنا الفكرية والسلوكية إلى جهات مختلفة، كلٌ حسب أهدافه واحتياجاته.

في مقابل هذه التهديدات، استعرض كُتّاب الرأي في الصحف السعودية منجزات المملكة في مجال الأمن السيبراني وحماية الخصوصية، مؤكدين أن الدولة حققت العديد من النجاحات في هذا المجال المهم والحيوي، خاصة بعد الاهتمام الكبير من جانب صاحب السمو الملكي الأمير محمد بن سلمان ولي العهد، حفظه الله، وحرصه على أهمية التقدم في مجال الأمن السيبراني؛ كونه متلازمًا مع عملية التحول الرقمي التي تنتهجها الدولة السعودية، وفق رؤية 2030 الطموحة.



الأطر المرجعية

استخدم كُتّاب الرأي عددًا من الأطر المرجعية خلال تناولهم للتهديدات السيبرانية وخطورتها على أمن وخصوصية المعلومات، علمًا بأنه كثيرًا ما اعتمد الكُتّاب على أكثر من إطار مرجعي في المقال الواحد، فجاءت نسب ظهورها متفاوتة، وذلك على النحو التالي:

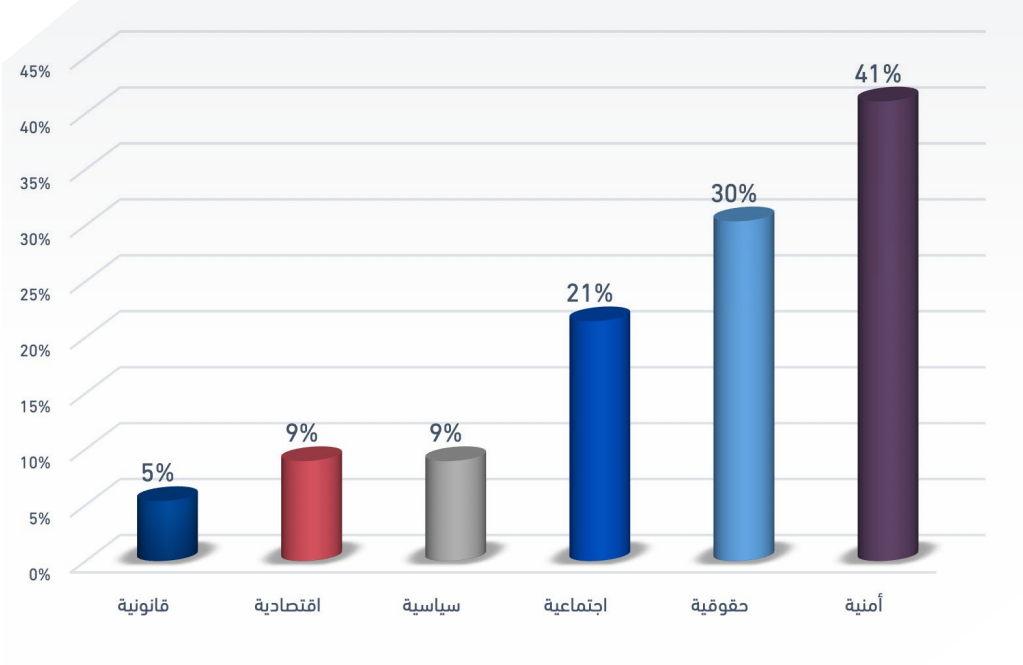
- تناول كُتّاب الرأي هذه القضية من **منظور أمني** في 41% من إجمالي عينة المقالات محل الدراسة، وذلك من خلال التركيز على التهديدات الأمنية التي قد يتعرض لها الأفراد أو المؤسسات أو الدول، وأكدت المقالات أن التهديدات الموجهة للأشخاص أو المؤسسات قد تتطور وتتحول إلى مخاطر تتعلق بالأمن القومي للدول، مُستعرضة العديد من الأمثلة المستقاة من وقائع سابقة كاستهداف شركات ومؤسسات أمريكية ولبنانية، فضلًا عن الاستهداف الذي تعرضت له شركة أرامكو السعودية ونجحت في التصدي له.

- وظهرت **المرجعية الحقوقية** بنسبة 30%، حيث أكد الكُتّاب على ضرورة احترام خصوصية المستخدمين، وحريتهم في الإفصاح من عدمه عن معلوماتهم الشخصية وخصوصيات حساباتهم، والتشديد على حقهم الأصيل في عدم استخدام بياناتهم دون موافقة صريحة وواضحة منهم.

- كما ظهرت **المرجعية الاجتماعية** في مجموعة من المقالات، إذ اهتمت بالقيم المجتمعية التي ترفض سلوكيات بعض المستخدمين على منصات التواصل الاجتماعي؛ كونها تتعارض مع عادات وتقاليد المملكة وشعبها المحافظ بطبعه، علاوةً على أنها تُسهل عملية اختراق خصوصية الأفراد. وشددت المقالات على أهمية دور الأسرة الرقابي بشأن استخدام الأطفال والمراهقين والشباب لوسائل التواصل الاجتماعي، وضرورة توعيتهم بمخاطر هذه المنصات، ومنها اختراق خصوصية الحسابات وسرقة البيانات الشخصية، وإمكانية استخدامها لأغراض تسويقية أو في الابتزاز المالي بعد إخضاعها لبعض الإجراءات التقنية.

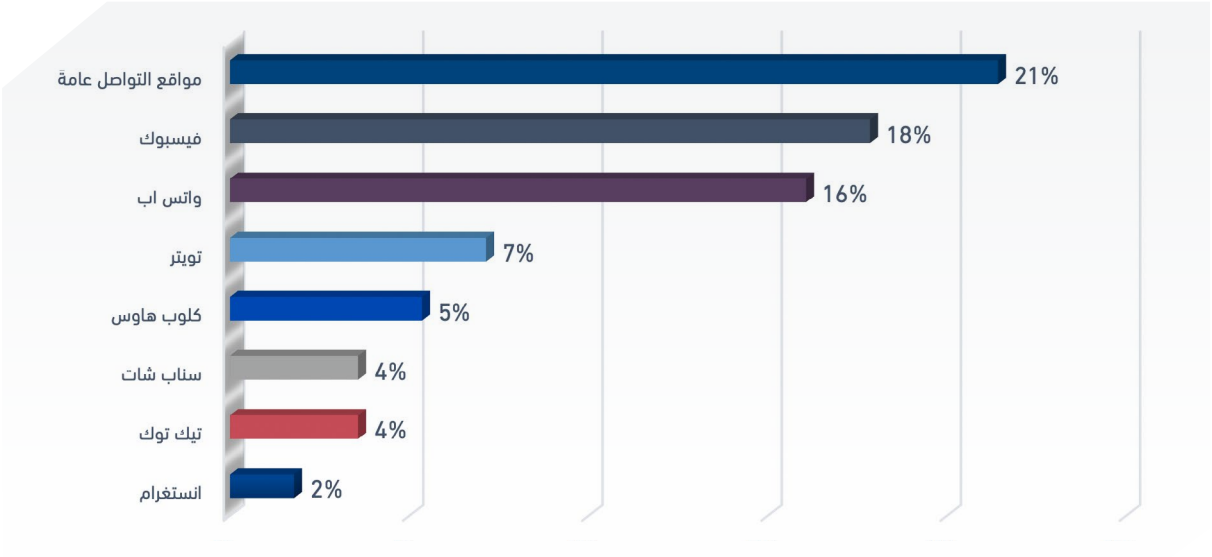
- أما **المرجعية السياسية** فكانت بنسبة 9% واعتمدت عليها مقالات الكُتّاب السعوديين حينما حذروا من لجوء بعض الأطراف، سواء كانت من قِبل جهات أو مؤسسات أو دول إلى استخدام بيانات المستخدمين وتوجهاتهم الفكرية والسلوكية؛ بهدف تحقيق مكاسب سياسية تتوافق مع أيديولوجيات ومصالح هذه الجهات، عبر التحكم والتوجيه السياسي، مثلما يحدث أثناء العمليات الانتخابية.

- وفيما يتعلق **بالمرجعية الاقتصادية** فجاءت أيضًا بنسبة 9%، إذ ركزت على تحوّل المنصات الاجتماعية إلى سوق إعلانية كبيرة، بفضل حجم البيانات الشخصية الضخم المتاح على هذه المنصات، الأمر الذي دفع الشركات إلى تسليع بيانات المستخدمين واستغلالها بشكل تجاري بحت بعيدًا عن أي اعتبارات أخلاقية أو قانونية.
- وظهرت **المرجعية القانونية** بنسبة 5% في مقالات كُتّاب الرأي السعوديين، حيث سعت إلى عرض نماذج من تجارب الدول الغربية لمواجهة التهديدات السيبرانية وانتهاك الخصوصية، مثل قيام دول الاتحاد الأوروبي بسن القوانين والتشريعات التي تُجرم الهجمات السيبرانية بجميع أشكالها، ومنها استهداف خصوصيات مستخدمي وسائل التواصل الاجتماعي، وإجبار الشركات على احترام خصوصية الأفراد.



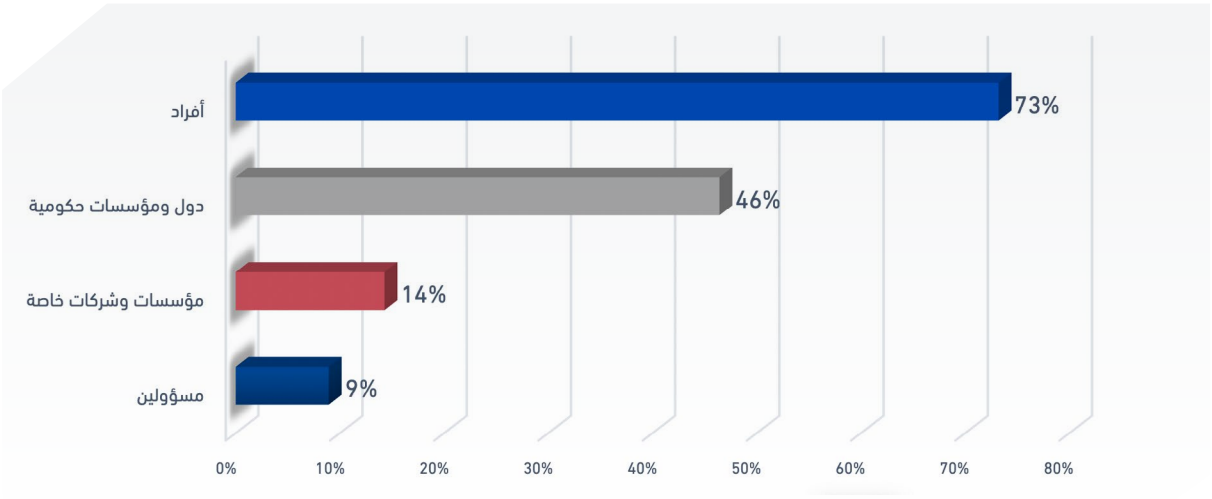
مصادر تهديد الخصوصية وأمن المعلومات

أبرز كُتّاب الرأي في مقالاتهم عددًا من المصادر التي يتم من خلالها تهديد واختراق خصوصية الأفراد والمؤسسات، وقد تصدرت هذه المصادر مواقع التواصل الاجتماعي، سواء تمت الإشارة لها بشكل عام أم بتحديد المنصات المُهدِّدة، التي جاء في مقدمتها فيسبوك و«واتساب»، ثم باقي المنصات على النحو المُوضَّح بالشكل البياني التالي:



وفي المرتبة الثانية ظهر الإنترنت - في المُطلق - كمصدر تهديد للخصوصية وأمن المعلومات، ثم الهواتف المحمولة (الذكية) خاصة هواوي وآبل، وأخيرًا ظهرت تطبيقات المتجر خاصة المجانية منها مثل تطبيق «زووم» على «جوجل بلاي»، وبالتساوي مع تطبيقات المتجر ظهرت المواقع الإلكترونية كمصدر تهديد للخصوصية وأمن المعلومات، ومن أمثلتها جوجل وأمازون.

الجهات الأكثر عُرضة للتهديد السيبراني



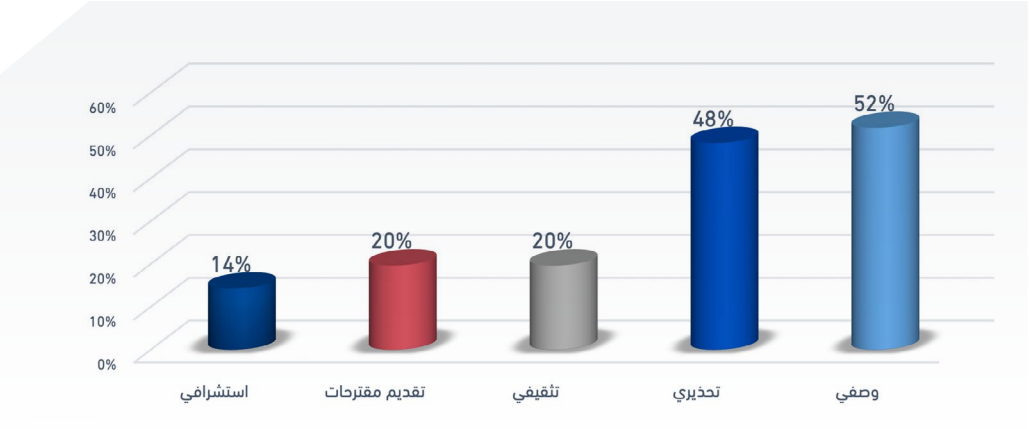
أظهرت النتائج تركيز كُتّاب المقالات على أربع جهات هي الأكثر عُرضة للتهديد السيبراني واختراق الخصوصية، جاء في مقدمتها «الأفراد» بنسبة ظهور بلغت 73%، وأرجعوا ذلك إلى كونهم الطرف الأكثر استخدامًا لوسائل التواصل الاجتماعي، والأكثر شغفًا بتحميل التطبيقات الإلكترونية، ولا يهتمون كثيرًا ببنود الخصوصية، بل يوافقون عليها بشكل تلقائي دون قراءتها، فضلًا عن عدم وعي وإدراك نسبة منهم بأهمية الحفاظ على خصوصيتهم، إضافة إلى عدم امتلاكهم التقنيات اللازمة لمنع عمليات الاختراق.

في المرتبة الثانية حلّت «الدول والمؤسسات الحكومية» بنسبة ظهور بلغت 46%، وأرجع الكُتّاب ذلك إلى الشكل الحالي للصراعات الدولية، والذي لم يعد مقتصرًا على المواجهات العسكرية، بل أصبح صراعًا قائمًا على الهجمات السيبرانية، وحروب المعلومات التي تُهدد المؤسسات وتستهدف الدول.

كما تطرق الكُتّاب إلى نوع آخر من الصراع، وهو الذي يحدث بين الشركات الخاصة حول امتلاك المعلومات والبيانات لاستخدامها واستغلالها في التنافس التجاري بهدف الاستحواذ على الأسواق.

إضافة إلى ذلك، أبرز كُتّاب المقالات أن المسؤولين الحكوميين لم يسلموا من الاستهداف والاختراق المعلوماتي؛ ليكونوا بمثابة مدخل إلى المؤسسة أو الوزارة التي يعملون بها، ومن ثمّ يسهُل اختراق الكيان سيبرانيًّا.

أسلوب التناول



اعتمد كُتّاب الرأي السعوديين على أكثر من أسلوب في معالجتهم للخصوصية وأمن المعلومات وخطورة التهديدات السيبرانية، وذلك على النحو التالي:

- جاء **الأسلوب الوصفي** في صدارة المعالجات، حيث ركّز على استعراض الوضع الراهن - محليًّا وعالميًّا - والمتعلق بالتهديدات السيبرانية وكيفية اختراق الخصوصية واستغلال بيانات المستخدمين، هذا من جانب، ومن جانب آخر الجهود المبذولة من جانب المملكة العربية السعودية للارتقاء والتميز في هذا المجال التكنولوجي والأمني الحيوي، والذي حققت فيه المملكة قفزات سريعة ونوعية، مع استعراض تطور وضع الأمن السيبراني في المملكة منذ شن الهجمات السيبرانية على شركة أرامكو في 2012 مرورًا بانطلاق رؤية 2030 ووصولًا إلى تحقق إنجاز الوصول إلى المركز الثاني عالميًّا عام 2021 لمؤشر الأمن السيبراني العالمي، كما أبرز هذا الأسلوب أيضًا دور مؤسسات

الدولة السعودية في حماية أمنها الوطني ضد الهجمات السيبرانية، وتوعية مواطنيها من السلوكيات الضارة بأمن معلوماتهم، وتحذيرهم من خطورة بعض التطبيقات التي تنتهك خصوصياتهم.

- حلّ **الأسلوب التحذيري** في المرتبة الثانية، وقد سعى الكُتّاب عبر هذا الأسلوب إلى تنبيه الجمهور من عمليات الاستغلال التي يتعرضون لها من خلال ما أُطلق عليه «الديكتاتورية الناعمة» التي تستخدمها مواقع التواصل الاجتماعي لاستقطاب المستخدمين، ومن ثمّ اختراق خصوصية بياناتهم واستغلالها سياسيًّا وتجاريًّا؛ وحذر كُتّاب الرأي في هذا الصدد بأن حروب المستقبل هي سيبرانية في المقام الأول، وأن الوطن العربي ليس بعيدًا عن الاستهداف، وهو ما يستوجب الحيطة والحرص سواء على المستوى الفردي أو الجماعي أو المؤسسي.
- أما **أسلوب التثقيف** فظهر في المرتبة الثالثة، وفيه حرص الكُتّاب على رفع مستوى وعي الجمهور، وتوسيع مداركه حول أهمية الخصوصية على الإنترنت، وضرورة الحفاظ على سرية البيانات الشخصية، فضلًا عن إعلامه بالحيل المختلفة التي تلجأ إليها المنصات الاجتماعية والتطبيقات الإلكترونية والشركات لانتهاك الخصوصية.
- وفيما يتعلق **بأسلوب تقديم المقترحات** الذي ظهر في المرتبة الرابعة، فلم يكتف كُتّاب المقالات في الصحف السعودية بتوصيف الحالة أو التحذير منها، وإنما سعوا إلى تقديم بعض الحلول – من وجهة نظرهم – والتي من شأنها المساهمة في تقليل خطورة الاستهداف والاختراق للخصوصية، ومنها على سبيل المثال لا الحصر العمل على حظر التطبيقات المنتهكة للخصوصية، وتدشين تطبيقات بديلة تتمتع بقدر أكبر من المهنية ومعايير الحماية والحصانة ضد الاختراق، وقيام الأجهزة المعنية في الدولة بسن التشريعات والقوانين التي تُجرم الهجمات السيبرانية بجميع أشكالها وتغليظ العقوبات ضد من يثبت تورطه فيها، مع ضرورة إيجاد شكل من أشكال التنسيق والتعاون الدولي، سواء في نقل المعرفة الخاصة بهذا المجال، أو التعاون لمواجهة هذا السلوك العدواني ضد الأفراد والمؤسسات.
- وظهر في المرتبة الخامسة **أسلوب الاستشراف**، والذي عُنِيَ بالتنبؤ بالمستقبل بناءً على المعطيات الراهنة، حيث يرى كُتّاب الرأي في الصحف السعودية أن العالم مُقدِم لا محالة على عهد جديد من الحروب يتمثل في الاعتداءات السيبرانية وانتهاك وتسليع الخصوصية، ولذلك فلا بديل عن التسلح بامتلاك أحدث التكنولوجيات التي تمنع أو تُحجم على أقل تقدير مخاطر هذه الاعتداءات، مع ضرورة رفع مستوى إدراك المواطنين بهذه المخاطر، وتوعيتهم بأفضل الطرق للحفاظ على خصوصياتهم وصونها من الاختراق.

الاستمالات الإقناعية

اعتمد كُتّاب الرأي في الصحف السعودية خلال تناولهم لقضية الخصوصية والأمن السيبراني على الاستمالات العقلية في المقام الأول بنسبة 55%، تلاها الاستمالات المختلطة التي تمزج بين العقلي والعاطفي بنسبة 24%، فيما جاء الاعتماد على الاستمالات العاطفية في المرتبة الثالثة بنسبة 21%.

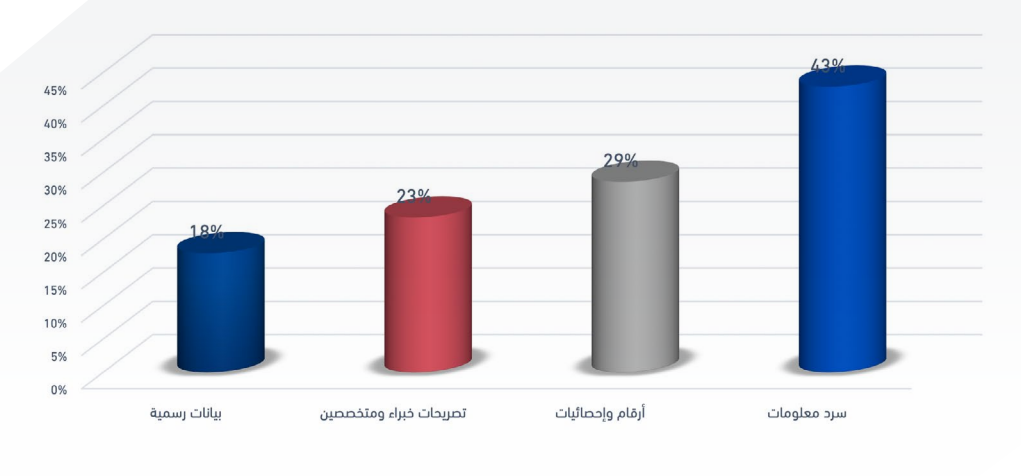
وتوضح هذه النتيجة أن النهج الإقناعي الذي اتبعه كُتّاب الرأي في مناقشتهم للقضية كان قائمًا على **المنطق ويُخاطب العقل** في الأساس، وهو ما يعني أنهم يمتلكون الأدلة والحُجج الفكرية التي تُثبت وتُبرهن أطروحاتهم التي تضمنتها مقالاتهم.

وتفصيليًّا.. تمثّلت أهم الاستمالات العقلية في **سرد المعلومات والاستشهادات** المبنية على التجارب الواقعية، ومن أمثلة ذلك عرض جهود المملكة في تعزيز منظومة أمنها السيبراني لتحقيق أكبر قدر من الحماية لخصوصية الأفراد والمؤسسات، كما استعرض الكُتّاب نماذج متعددة لهجمات سيبرانية تعرضت لها دول ومؤسسات مختلفة حول العالم.

في المرتبة الثانية ظهر **استخدام لغة الأرقام** والإحصاءات، حيث لجأ الكُتّاب إلى الاستشهاد بتقارير المنظمات والمؤسسات الدولية، كتلك التي تناولت النجاحات والإنجازات التي حققتها المملكة العربية السعودية في مجال الأمن السيبراني، واحتلالها مراتب متقدمة على الصعيد العالمي، كما تم استخدام الأرقام والإحصاءات لإبراز الآثار الاقتصادية السلبية الناتجة عن اختراق خصوصية البيانات والمعلومات، فضلًا عن الإحصاءات المتعلقة بنسب عمليات الاختراق حول العالم، وتلك المتعلقة بحجم من يهتمون بمراجعة بنود الخصوصية مقارنة بمن يتجاهلونها.

أما **تصريحات الخبراء والمتخصصين** في مجال الأمن السيبراني، فقد اعتمد عليها الكُتّاب لتوضيح أهمية البيانات في العصر الحالي مما جعلها مصدر جذب للمستغلين الذين يستهدفون الربح حتى وإن كان على حساب خصوصية وأمن الآخرين، واستخدم كُتّاب المقالات تحذيرات هذه الفئة المتخصصة في الأمن السيبراني لإظهار مدى الاستهداف الذي يمكن أن يتعرض له الأفراد والمؤسسات.

وأخيرًا ، حلّت **البيانات الرسمية** الصادرة عن مؤسسات الدولة أو المؤسسات والدول الأجنبية، وقد تضمنت في أغلبها محتويات تحذيرية حول أساليب اختراق وانتهاك الخصوصية والعوامل المساعدة التي تُسهّل من عملية الاختراق، إضافة إلى الإعلان عن التطبيقات والتحديثات التي قد تتسبب في تهديد خصوصية المستخدمين، كما حملت هذه الفئة مضامين توعوية تُقدم نصائح وإرشادات تتعلق بكيفية الحفاظ على أمن المعلومات من أي تهديد مُحتمل.



أما الاستمالات العاطفية التي اعتمد عليها كُتّاب الرأي السعوديين فتمثّلت في ظهور **أسلوب الترهيب**، وذلك من خلال تركيزهم على إثارة مشاعر الخوف لدى المستخدمين، بهدف حثّهم على زيادة الاهتمام بالحفاظ على أمن وخصوصية معلوماتهم، واتخاذ كافة الإجراءات الكفيلة لمنع اختراقها، ولذلك حرص الكُتّاب على إبراز المخاطر التي قد يتعرض لها المستخدمون وخاصة لوسائل التواصل الاجتماعي، ومن الاستشهادات على ذلك:

- وسائل التواصل الاجتماعي قادرة على الاستماع إليك ليلًا ونهارًا، ومعرفة أفكارك، وميولك في الطعام والشراب، ونبرة صوتك، ووجهك.
- المنصات الاجتماعية تحظى بما لم يحظَ به جهاز مخابرات مهما بلغت قوته.
- تُعد بياناتك كمستخدم للتقنية سلعة ثمينة، لأنها بشكل أو بآخر تستخدم كأداة تأثير لك أو عليك.
- الأطفال والنساء من أكثر الفئات المستهدفة لتهديدات الفضاء الإلكتروني.
- الأضرار الاقتصادية للهجمات السيبرانية تماثل أضرار الحروب التقليدية.
- بعض الهجمات السيبرانية يتم تمويلها من جانب الدول الخارجية التي تمارس الإرهاب الدولي.

وفي هذا الصدد، استخدم كُتّاب الرأي مجموعة من المصطلحات والعبارات الوصفية التي تعكس هذه المخاطر، مثل (الهلع، الخوف، القلق، التحذير، الحروب السيبرانية، تجسس الأجهزة المخابراتية، ملاحقتك أمنيًّا، قد يبتلعك الوحش).

في المرتبة الثانية ظهرت استمالة **الحاجة إلى الأمان**، حيث سعى كُتّاب الرأي إلى التأكيد على ضرورة حماية أنفسنا في الفضاء الرقمي، وربطوا بين استخدام وسائل الاتصال الحديثة وعلى رأسها منصات التواصل الاجتماعي وبين تراجع درجة الأمان المتوفرة للشخص.

كما ربط كُتّاب الرأي بين انتهاك الخصوصية الفردية وتأثيره على الخصوصية المجتمعية، إذ إنه في بعض الحالات تلجأ أطراف خارجية إلى اختراق خصوصية الأفراد من أجل استكشاف المزاج العام للمجتمع ككل، واهتماماته وشواغله، ومن ثمّ استخدام هذه النوعية من المعلومات في استهداف الدول أو المجتمعات. ولذلك أكد الكُتّاب على أهمية الدور الشخصي في الحفاظ على أمن واستقرار البيئة المحيطة.

الحاجة للأمان

%18

الترهيب

%27

أطر التناول

كشفت نتائج التحليل أن كُتّاب الرأي السعوديين استخدموا مجموعة من الأطر خلال تناولهم لقضية الخصوصية والأمن السيبراني، وذلك على النحو التالي:

1. إطار المسؤولية: تم استخدامه في إبراز:

- دور الأفراد في حماية خصوصيتهم على مواقع التواصل الاجتماعي وتطبيقات الهواتف الجوالة، وأهمية التأكد من بنود الخصوصية وشروط الاستخدام.
- دور الأسرة في تربية الأطفال والمراهقين، وتوعيتهم بأهمية الحفاظ على خصوصية البيانات.
- دور الدول ومؤسساتها في حماية الخصوصية والأمن المعلوماتي، والتسلح بأحدث الأدوات التكنولوجية لمواجهة التهديدات الإلكترونية والسيبرانية، وسنّ القوانين التي تحمي الخصوصية الفردية والوطنية.

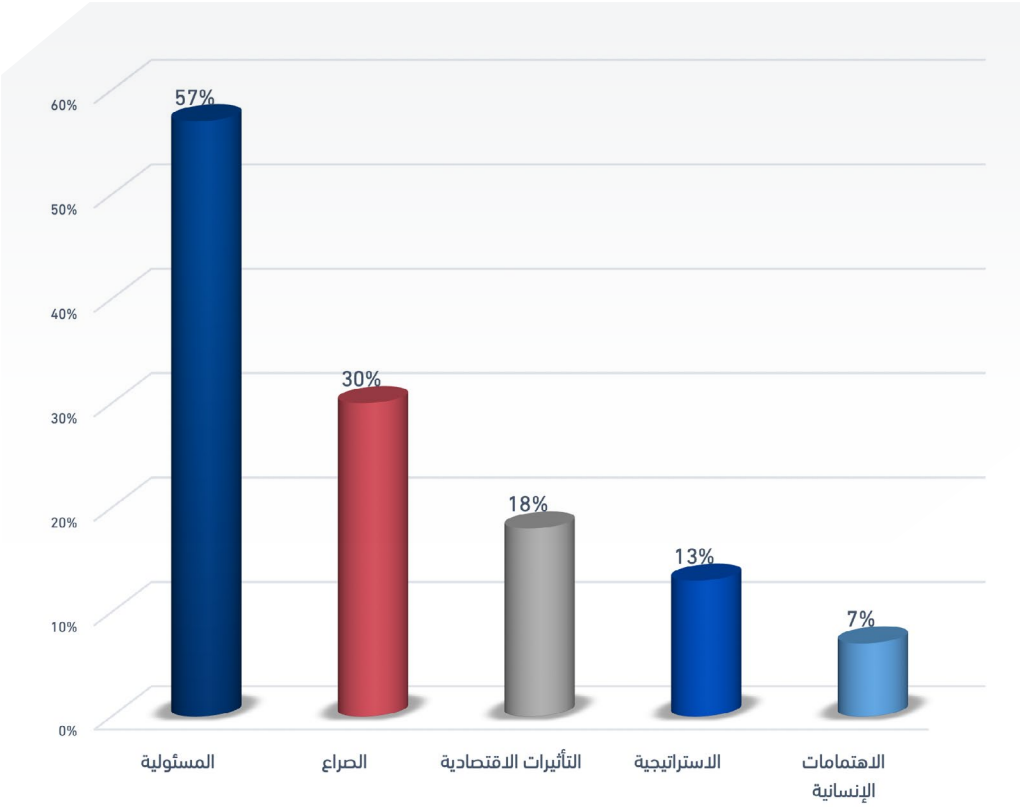
2. **إطار الصراع:** حيث تناولت بعض مقالات الرأي قضية الخصوصية والأمن السيبراني من منظور الصراع الحالي والمستقبلي، والمتمثل في:

- الحروب السيبرانية والصراع الخفي والمعلن بين الدول عبر استخدام بيانات المستخدمين للتكنولوجيا والتطبيقات الإلكترونية.
- الصراع بين الحاجة إلى التحول الرقمي، وزيادة التعرض لمخاطر انتهاك الخصوصية كنتيجة مرتبطة بهذا التحول.
- الصراع الاقتصادي والتقني بين الشركات التكنولوجية، والذي يتخذ عدة أشكال، منها استعراض كل شركة لقدراتها في حماية بيانات مستخدميها، وفي المقابل صراع الشركات على الاستحواذ على بيانات المستخدمين واستغلالها تجاريًّا (تسليع البيانات) بهدف تحقيق مكاسب مادية.
- الصراع الداخلي لبعض المستخدمين بين رغبتهم الجامحة في تحقيق الشهرة من جانب، وما يستلزمه من تهاون أو تساهل في أمن بياناتهم وخصوصيتهم من جانب آخر.

3. **إطار التأثيرات الاقتصادية:** وفيه تم التركيز على إبراز الخسائر المالية واللوجستية التي تتعرض لها المؤسسات والدول نتيجة الاختراقات السيبرانية وانتهاك خصوصية البيانات، وأيضًا المكاسب التي تُحققها الجهات المُخترقة نتيجة بيع بيانات المستخدمين، أو تلك المتحققة عبر المطالبات بالفدية المالية مقابل عدم نشر البيانات الخاصة أو بيعها لجهات منافسة.

4. **إطار الاستراتيجية:** حيث تناول كُتّاب الرأي السعوديين القضية من منظورها الاستراتيجي، خاصة فيما يتعلق بكيفية مواجهة التهديدات السيبرانية واختراق خصوصية البيانات، وذلك عبر استعراض مجموعة من الإجراءات والخطوات المهمة والضرورية، مثل توعية وتثقيف المواطنين بأهمية الحفاظ على أمن وخصوصية بياناتهم الرقمية، وضرورة اهتمام الدولة بإيجاد بدائل للبرامج والتطبيقات الإلكترونية تكون عالية الحماية للبيانات بحيث يتم استخدامها في المؤسسات والجهات الحكومية، فضلًا عن أهمية قيام مؤسسات الدولة المعنية بوضع خارطة طريق تستهدف تحقيق أكبر قدر من الحماية لخصوصية الأفراد والمؤسسات.

5. **إطار الاهتمامات الإنسانية:** وفيه أوضح الكُتّاب أن الكثير من الشركات المالكة للتطبيقات ومنصات التواصل تستغل اهتمامات المستخدمين بشكل انتهازي، وذلك من خلال إغرائهم بالمميزات التي توفرها والحوافز المتحققة لهم نتيجة الانضمام إليها، وأنه بمجرد انضمامهم يُصبحون بمثابة فريسة سائغة لانتهاك خصوصيتهم، والحصول على بياناتهم ومعلوماتهم الشخصية.



ثانياً

تحليل مضمون حساب «الهيئة الوطنية للأمن السيبراني» على تويتر

أما على مستوى الرسائل الاتصالية الصادرة عن المؤسسات والهيئات الرسمية في المملكة العربية السعودية بشأن قضية الخصوصية والأمن السيبراني، فقد قامت الدراسة بتحليل حساب الهيئة الوطنية للأمن السيبراني على تويتر، الذي يُعرّف نفسه في النبذة التعريفية الخاصة به على أنه «الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه ودعمه وتعزيزه».

وحسب الموقع الرسمي للهيئة، فقد جاء تأسيسها انطلاقًا من إدراك وتفاعل المملكة العربية السعودية مع مستجدات العصر وتطوراته، وترجمةً لنهج خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وصاحب السمو الملكي الأمير محمد بن سلمان ولي العهد - حفظهما الله - في قيادة المملكة لتكون نموذجًا ناجحًا ورائدًا في العالم على كافة الأصعدة، وانعكاسًا لرؤية المملكة 2030 التي جعلت التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية ضمن مستهدفاتها، واستشعارًا لأهمية البيانات والأنظمة التقنية والبُنى التحتية الحساسة وارتباطها بالمصالح الوطنية، وأهمية حمايتها من أي تهديدات أو مخاطر يشهدها الفضاء السيبراني.

ويعكس تأسيس الهيئة الوطنية للأمن السيبراني وارتباطها بالملك - حفظه الله - وفق الأمر الملكي الكريم بالموافقة على تنظيمها بتاريخ 1439/2/11هـ، مدى الأهمية التي توليها القيادة الرشيدة بهذا المجال، وذلك حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبُنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

وبناءً على ذلك، جاءت اختصاصات الهيئة متعددة ومتنوعة، ومنها على سبيل المثال لا الحصر:

- إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها، واقتراح تحديثها.
- وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها.
- تصنيف وتحديد البُنى التحتية الحساسة والجهات المرتبطة بها، وتحديد القطاعات والجهات ذات الأولوية بالأمن السيبراني.
- بناء مراكز العمليات الوطنية الخاصة بالأمن السيبراني – وما في حكمها –

بكافة أنواعها، بما في ذلك مراكز التحكم والسيطرة والاستطلاع والرصد وتبادل وتحليل المعلومات، وكذلك بناء مراكز العمليات القطاعية الخاصة بالأمن السيبراني – عند الحاجة - وبناء المنصات ذات العلاقة، والإشراف عليها، وتشغيلها.

- بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة.
- التواصل مع الجهات المماثلة خارج المملكة والجهات الخاصة لتبادل الخبرات، وتأسيس آليات للتعاون والشراكة معها، وفقاً للإجراءات المتبعة.
- رفع مستوى الوعي بالأمن السيبراني.
- تحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.
- اقتراح إصدار وتعديل الأنظمة واللوائح والقرارات ذات الصلة بالأمن السيبراني.

ويتضح من هذه الاختصاصات تركيز الهيئة الوطنية للأمن السيبراني على محورين مركزيين هما تعزيز قدرات المملكة في مجال الأمن السيبراني لمواجهة كافة أنواع التحديات والمخاطر المتعلقة به، هذا من جانب، ومن جانب آخر بناء القدرات الوطنية المتخصصة في مجال الأمن السيبراني، بحيث تكون هناك كوادر سعودية مؤهلة علميًّا وعمليًّا وفق أحدث النظم المعمول بها عالميًّا.

ونظرًا لأهمية الأمن السيبراني خاصة مع الاستخدام الجماهيري الضخم والمتزايد للإنترنت ووسائل التواصل الاجتماعي في شتى مناحي الحياة، فإن التواصل مع الجمهور يُعد أحد العوامل الرئيسية المساهمة في تحقيق الأهداف الاتصالية للهيئة.

ولضمان الوصول ومخاطبة أكبر شريحة من الجمهور، تم إنشاء حساب للهيئة الوطنية للأمن السيبراني على منصة «تويتر» في ديسمبر 2017م، حيث يقترب عدد المتابعين للحساب من 260 ألف متابع، فيما يبلغ إجمالي تغريداته (572) تغريدة، وذلك حتى وقت إجراء الدراسة.

ومن أجل التعرف على طبيعة الرسائل الاتصالية التي يُقدمها حساب الهيئة كمُمثل للمؤسسات والهيئات الحكومية المعنية بمجال الأمن السيبراني، قامت الدراسة برصد وتحليل عينة عمدية قوامها (200) تغريدة «أصلية» تم نشرها في الحساب خلال الفترة الممتدة من أول يوليو 2020م، وحتى نهاية أغسطس 2021م.

وقد انتهت النتائج إلى ما يلي:

أهداف التغريد

يهتم حساب الهيئة الوطنية للأمن السيبراني على تويتر باستعراض الدور الذي تقوم به الدولة السعودية في سبيل تعزيز أمنها الوطني السيبراني، وتحقيق أقصى درجات الحماية، سواء لمؤسسات الدولة أو للأفراد أو للمصالح الحيوية في المملكة.

وانطلاقًا من ذلك، فقد أظهرت نتائج التحليل أن محتوى تغريدات الحساب تضمن ثلاثة أهداف أساسية، نستعرضها على النحو التالي:

1. إبراز جهود وإنجازات المملكة في مجال الأمن السيبراني

حلّ هذا الهدف في المرتبة الأولى بنسبة 58.5%، وفيه تبنى حساب الهيئة الوطنية للأمن السيبراني لغة خطاب تحمل الكثير من الفخر والاعتزاز بما تُحققه المملكة من نجاحات وإنجازات، وما وصلت إليه من مكانة في مجال الأمن السيبراني، ليس على المستوى العربي والإقليمي فحسب، بل وعلى الصعيد العالمي أيضًا، وذلك بحصولها على المركز الثاني عالميًا في الأمن السيبراني.

وفي هذا الصدد، حرص حساب الهيئة على توجيه الشكر والعرفان لمقام خادم الحرمين الشريفين الملك سلمان بن عبد العزيز ولصاحب السمو الملكي الأمير محمد بن سلمان ولي العهد – حفظهما الله – لسياساتهما الداعمة بكل قوة لمجال الأمن السيبراني في المملكة. كما أبرز الحساب الإشادات الدولية التي تناولت مبادرة سمو ولي العهد الأمير محمد بن سلمان لتوفير الحماية والتمكين للأطفال في الفضاء السيبراني.

إضافة إلى ذلك، استعرض حساب الهيئة الوطنية للأمن السيبراني على تويتر جهوده في إطار تعزيز منظومة الأمن السيبراني في المملكة، ومنها:

- توقيع الهيئة اتفاقية شراكة استراتيجية مع وكالة الأمم المتحدة لإطلاق البرنامج العالمي لحماية وتمكين الأطفال في الفضاء السيبراني.
- توقيع اتفاقية تعاون بين الهيئة الوطنية للأمن السيبراني ووزارة التعليم بهدف رفع جودة مخرجات البرامج التعليمية ومواءمتها مع الاحتياجات الوطنية ودعم وتشجيع الأبحاث وتأهيل الكوادر وتطوير المهارات ونشر التوعية في مجال الأمن السيبراني.
- ساهمت جهود الهيئة الوطنية للأمن السيبراني وشركة سايت خلال موسم حج 1442هـ في تعزيز جانب الأمن السيبراني من خلال مراقبة الفضاء السيبراني ورصد التهديدات السيبرانية، ورفع جاهزية استجابة الجهات الوطنية للحوادث السيبرانية.

- ساهمت الهيئة في دعم وتعزيز القدرات الوطنية من خلال توفير الفرص التدريبية للشباب في مجالات الأمن السيبراني.
- تعمل الهيئة الوطنية للأمن السيبراني على الوصول إلى فضاء سيبراني سعودي آمن وموثوق يمكّن من النمو والازدهار.
- إصدار الهيئة الوطنية للأمن السيبراني (ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات).
- إعداد إطار «سايبر التعليم» ليكون متوافقاً مع التصنيف السعودي الموحد للمستويات والتخصصات التعليمية والإطار الوطني للمؤهلات، حيث يهدف هذا الإطار إلى المساهمة في وضع الحد الأدنى من متطلبات الخطط الدراسية لبرامج التعليم العالي في الأمن السيبراني.

2. تحفيز وتشجيع المواطنين ليُصبحوا كوادر مؤهلة في مجال الأمن السيبراني

جاء هذا الهدف في المرتبة الثانية بنسبة 30.5%، وفيه اتبع حساب الهيئة الوطنية للأمن السيبراني أسلوب تغريد يُحفز المستخدمين على التفاعل والمشاركة مع رسائله الاتصالية، مثل إقامة (#تحدي_الأمن_السيبراني) والذي يُمثل نواة لمبادرة تنمية سوق وصناعة الأمن السيبراني في المملكة، ويستهدف توطين تقنيات الأمن السيبراني والمساهمة الاقتصادية وخلق الوظائف وزيادة عدد شركات الأمن السيبراني الناشئة في المملكة، فضلًا عن تمكين المواهب الوطنية.

وتسعى الهيئة من خلال هذا النموذج الاتصالي إلى جذب السعوديين سواء كانوا أفرادًا أو شركات ناشئة للمشاركة في مجال الأمن السيبراني، ومن الاستشهادات على ذلك:

- بادر بالاستفادة من ورشة العمل المقدمة حول تحدي الأمن السيبراني وخطوات إطلاق المشاريع الريادية في مجال الأمن السيبراني.
- شاركنا بآرائك المتجددة في تحدي الأمن السيبراني.
- ساهم في صناعة مستقبل الأمن السيبراني من خلال مشاركتك في تحدي الأمن السيبراني.
- كن شريك المستقبل وساهم بآرائك وتطلعاتك في تطوير التحول الرقمي للمنصات الحكومية من خلال المشاركة في استبيان هيئة الحكومة الرقمية حول المنصات والخدمات الرقمية.
- حان الوقت لتساهموا في إيجاد فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار.

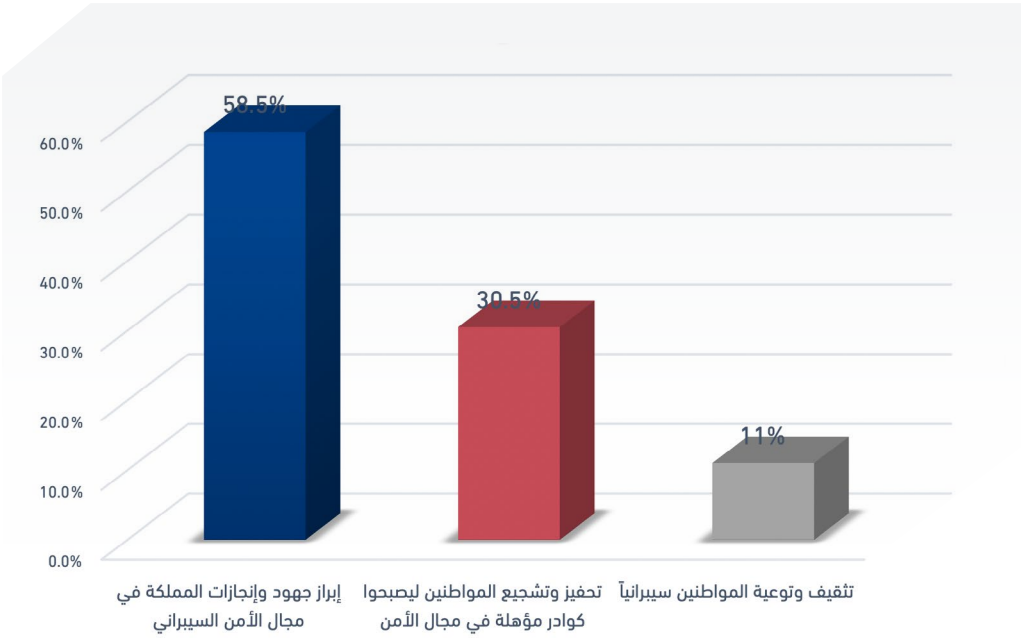
- هذا بالإضافة إلى الإعلان عن ورش العمل والمحاضرات والمبادرات التي تنظمها الهيئة الوطنية للأمن السيبراني على الإنترنت، مثل «مبادرة التدريب للتأهيل للتوظيف (CyberPro+)» حيث شارك فيها المتدربون على تمارين سيبرانية تنفذها شركة سايت لمحاكاة الهجمات السيبرانية، والتطبيق العملي لاكتشافها والاستجابة لها ومواجهتها.

3. تثقيف وتوعية المواطنين سيبرانيًّا

احتلّ هذا الهدف المرتبة الثالثة بنسبة 11%، وفيه تم التركيز على تأكيد أهمية الحفاظ على الخصوصية، والتعريف بمصطلحات ومجالات الأمن السيبراني ومخاطره؛ وقد اعتمد حساب الهيئة الوطنية للأمن السيبراني في ذلك على الوسائط الإلكترونية وخاصة الإنفوجرافيك من أجل تبسيط المعلومات المعقدة وإيصالها للمتلقي بسهولة ويُسر.

واتبع حساب الهيئة أسلوبًا استفهاميًّا في أغلب التغريدات التي تناولت هذا الهدف وذلك لإثارة الانتباه. فجاء نص التغريدة على شكل سؤال، أما الإجابة فكانت عبارة عن إنفوجرافيك أو فيديوجرافيك وغيرهما من وسائط. ومن أمثلة ذلك:

- ما هو صمود الأمن السيبراني؟
- نسمع عن أثر الهجمات السيبرانية... ونتساءل ... هل هو افتراضي أو واقع؟
- ما هي مجالات الأمن السيبراني؟



القوى الفاعلة

كشفت نتائج التحليل ظهور عدد من القوى الفاعلة في تغريدات الحساب محل الدراسة، حيث تصدرت مؤسسات الدولة هذه القوى بنسبة 59%، تلاها في المرتبة الثانية المملكة سواء ككيان عام أو مُمثلة في القيادة الرشيدة، حفظها الله، بنسبة ظهور بلغت 19%، ثم الكوادر الوطنية في المرتبة الثالثة بنسبة ظهور 6%، واللافت أن الأدوار المنسوبة إلى جميع هذه القوى اتسمت بالإيجابية، وتمثّلت أهم هذه الأدوار فيما يلي:

أولاً: مؤسسات الدولة: حيث أبرز الحساب مؤسسات الدولة كجهة تنفيذية لاستراتيجية المملكة المتعلقة بمجال الأمن السيبراني، وجهودها المتواصلة من أجل تعزيز مكانة المملكة سيبرانيًّا على الصعيد العالمي، وعملها المستمر من أجل الحفاظ على أمن المعلومات سواء للمؤسسات أو الأفراد. ومن أمثلة المؤسسات التي ركز عليها الحساب (الهيئة الوطنية للأمن السيبراني، هيئة الحكومة الرقمية، ومجلس الوزراء).

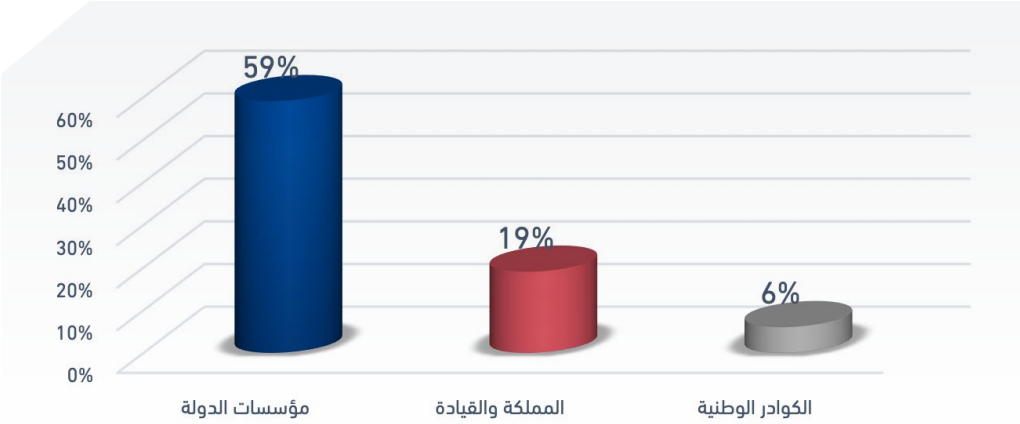
وقد تمحورت الأدوار المنسوبة لمؤسسات الدولة فيما يلي:

- دعم وتعزيز القدرات الوطنية من خلال توفير الفرص التدريبية للشباب.
- تشجيع المواطنين والشركات الناشئة للانخراط في مجال الأمن السيبراني.
- تعزيز الأمن السيبراني من خلال مراقبة الفضاء السيبراني ورصد التهديدات السيبرانية ورفع جاهزية الاستجابة للجهات الوطنية تجاه الحوادث السيبرانية.
- المساهمة الفعّالة في بناء مجتمع رقمي وتسريع عملية التحول الرقمي في المملكة.
- تنظيم ورش عمل توعوية تتناول الإرشادات الخاصة بالأمن السيبراني.
- التشجيع والتحفيز على الاشتراك في مبادرة التدريب للتأهيل للتوظيف.
- العمل على حماية المصالح الوطنية، ودعم أهداف رؤية السعودية 2030 الطموحة التي عزّزت التحول الرقمي، وجعلت من المملكة نموذجًا متميزًا ورائدًا في العالم.

ثانيًا- المملكة والقيادة الرشيدة: تناول الحساب هذه القوى من منظور الإطار الاستراتيجي للدولة السعودية، حيث تم استعراض دورها من خلال إبراز جهود المملكة «ككيان» في مجال تعزيز الأمن السيبراني، إضافة إلى سياسات وتوجيهات القيادة الرشيدة التي تبنّت التحول الرقمي كهدف رئيسي ضمن رؤية المملكة 2030، وقناعتها بأن هذا التحول يتطلب بالضرورة تعزيز القدرات السيبرانية للمملكة، ولذلك جاء دعمهما الكامل لهذا المجال الحيوي.

وأوضح حساب الهيئة الوطنية للأمن السيبراني أن سياسات وتوجيهات القيادة الرشيدة، حفظها الله، أسفرت عن انطلاق المملكة بخطى ثابتة واستراتيجية محكمة نحو فضاء سيبراني آمن وموثوق، جعلها تصعد إلى المركز الثاني عالميًّا في المؤشر العالمي للأمن السيبراني، واستعرض الحساب رجع الصدى الدولي حول المملكة والمتمثل في الإشادة بجهودها في هذا المجال.

ثالثًا- الكوادر الوطنية: تم تناولها من منطلق كونها من المخرجات المستهدفة للجهود السعودية المبذولة في مجال الأمن السيبراني، حيث تسعى المملكة لتوطين تقنيات الأمن السيبراني وخلق الوظائف وتمكين المواهب الوطنية؛ لبناء كوادر سعودية مؤهلة ومتميزة في مجالات الأمن السيبراني.

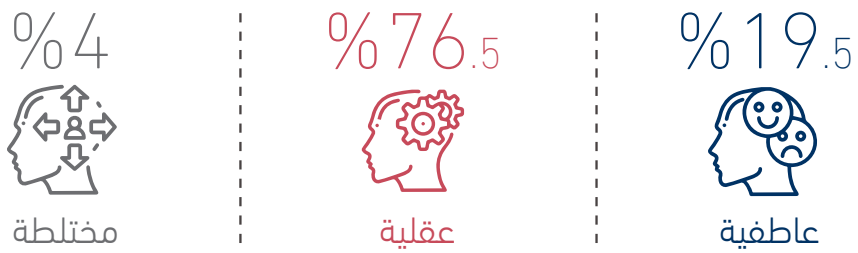


الاستمالات الإقناعية

أظهرت النتائج أن حساب الهيئة الوطنية للأمن السيبراني استخدم في المقام الأول الاستمالات العقلية لإقناع المستخدمين برسائله الاتصالية، وذلك بنسبة 76.5%، وقد تمثّلت أبرز هذه الاستمالات في البيانات الصادرة عن المؤسسات الرسمية المحلية والدولية، تلاها تصريحات المسؤولين، ثم جاء الاعتماد على لغة الأرقام والإحصاءات، علمًا بأن الأخيرة كان يتم استخدامها أيضًا في البيانات والتصريحات.

أما الاستمالات العاطفية فحلّت بالمرتبة الثانية بنسبة 19.5%، وفيها تم التركيز على استثارة همم السعوديين من خلال تشجيعهم وتحفيزهم للمشاركة الفعّالة في مجالات الأمن السيبراني، وإثارة مشاعر الفخر والاعتزاز بقدرات وإمكانات الوطن والمواطنين، فضلًا عن الفخر والتباهي بسمو ولي العهد، حفظه الله، فغرد الحساب قائلًا: «حق لنا اليوم أن نُفاخر ونُباهي بقائد عظيم، ننطلق بهمته ورؤيته لغد مشرق، وتحقيق المزيد من الرفعة والازدهار».

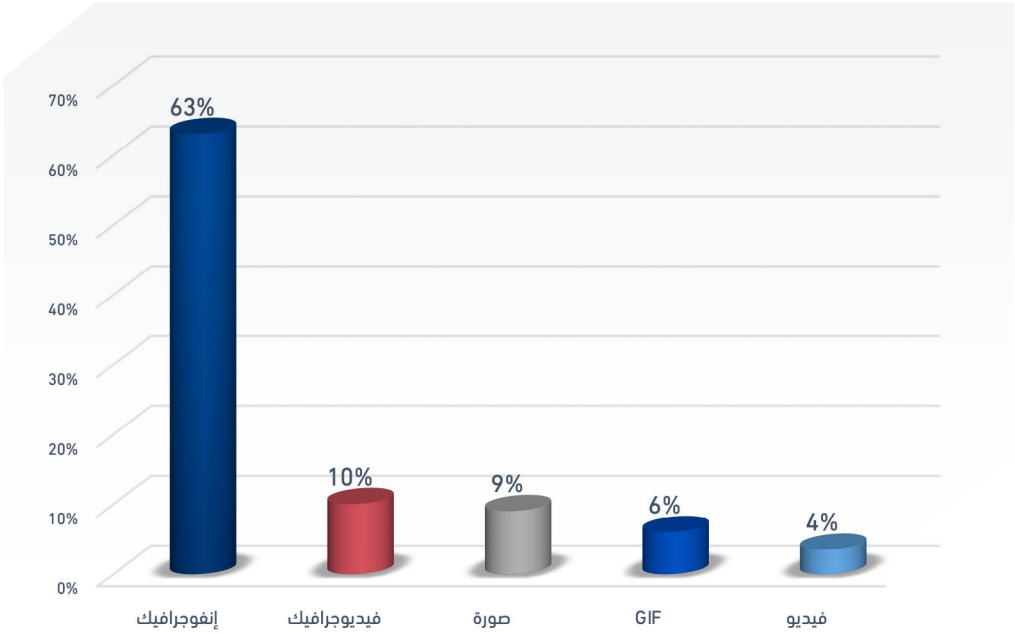
وفي المقابل، سعى الحساب أيضًا لاستثارة عاطفة الخوف والترهيب عبر تحذير المستخدمين من خطورة الهجمات السيبرانية التي قد تستهدفهم.



الأدوات الرقمية

استخدم حساب الهيئة الوطنية للأمن السيبراني الوسائط الرقمية في الغالبية العظمى من تغريداته عينة الدراسة وذلك بنسبة 92%، مقابل 8% جاءت نصية فقط. وقد تصدر الإنفوجرافيك ثم الفيديوجرافيك هذه الوسائط، حيث اعتمد عليهما الحساب بهدف تبسيط المعلومات والأرقام وإيصال رسائله الاتصالية بسهولة ويُسر، وبشكل جذاب ولافت.

أما فيما يتعلق بالصور والفيديوهات فتم الاعتماد عليهما لإبراز وتوثيق الفعاليات والأنشطة والأحداث المتعلقة بعمل الهيئة؛ مثل الدورات والمبادرات التي تقوم بها.

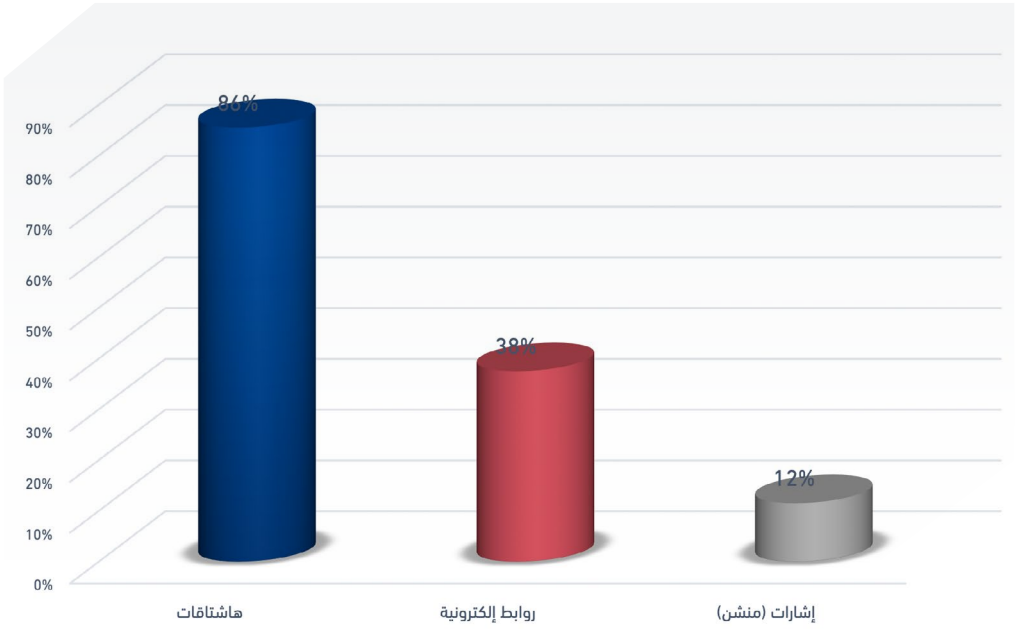


وبالنسبة لمدى الاعتماد على أدوات الانتشار الرقمي، فقد كشفت النتائج حرص الحساب على استخدام تلك الأدوات وخاصة الهاشتاق الذي ظهر في 86% من إجمالي تغريدات الدراسة، وكان من الملاحظ أن حساب الهيئة لجأ إلى تدشين هاشتاقات خاصة بالمبادرات والفعاليات التي تقوم بها الهيئة الوطنية للأمن السيبراني، فضلًا عن استخدام هاشتاقات باللغتين العربية والإنجليزية مرتبطة موضوعيًّا ومؤسسيًّا بمجالات عملها، وذلك من أجل إبراز التجربة السعودية الرائدة في مجال الأمن السيبراني للداخل والخارج.

ومن أمثلة الهاشتاقات التي تكررت في التغريدات (#تحدي_الأمن_السيبراني، #السعودية_سيبرانيا_الثانية_عالميا، #هيئة_الحكومة_الرقمية-، #الهيئة_الوطنية_للأمن_السيبراني، #المنتدى_الدولي_للأمن_السيبراني، #OnlineSaftey، #SafeOn-line، #cybersecurity، NCA، #NCA_KSA، #فضاء_سيبراني_ آمن_للأطفال، #الاستيراتيجية_الوطنية_للأمن_السيبراني، #أدوات_الأمن_السيبراني، #فضاء_سيبراني_سعودي_آمن).

وفي المرتبة الثانية جاءت الروابط الإلكترونية بنسبة ظهور بلغت 38%، وكان أبرزها رابط الموقع الإلكتروني للهيئة الوطنية للأمن السيبراني على الإنترنت، مما يعكس حرص الهيئة على إحداث نوع من التكامل والترابط بين حساباتها على المنصات المختلفة.

كما حرص الحساب على استخدام أداة الإشارة (منشن) والتي ظهرت في 12% من التغريدات عينة الدراسة، حيث جاء اعتماد الحساب على هذه الأداة؛ ليعكس من جهة حالة التضافر بين مؤسسات الدولة التي تتعاون من أجل تعزيز الأمن السيبراني، ومن جهة أخرى لإبراز الشراكات الاستراتيجية والتعاون مع المؤسسات الدولية في هذا المجال، ومن أمثلة الجهات التي تمت الإشارة لها في الحساب (وزارة التعليم العام، المركز الوطني الإرشادي للأمن السيبراني، المكتب الإقليمي العربي للاتحاد الدولي للاتصالات، الأمين العام للاتحاد الدولي للاتصالات، الشركة السعودية لتقنية المعلومات- سايت، الهيئة العامة للمنشآت الصغيرة والمتوسطة – منشآت، صندوق تنمية الموارد البشرية – هدف، المنتدى العالمي للأمن السيبراني، ومركز ذكاء).



ثالثًا

تحليل طبيعة تفاعلات المستخدمين السعوديين حول قضية الخصوصية المعلوماتية ومدى إدراكهم لأهمية الأمن السيبراني

سعت الدراسة لاستكشاف انطباعات المستخدمين السعوديين حول الخصوصية المعلوماتية ومدى إدراكهم لأهمية الأمن السيبراني، وذلك من خلال رصد وتحليل عينة عمدية لتفاعلاتهم على تويتر بشأن هذه القضية، علمًا بأن العينة بلغت (200) تغريدة تم نشرها خلال المدى الزمني 2020 – 2021م، وقد تم استخراجها باستخدام هاشتاقات وكلمات بحثية تمثلت في (هاشتاق #الخصوصية) ومصطلحي (الخصوصية، الأمن السيبراني)، **وقد انتهت نتائج التحليل إلى ما يلي:**

التأطير

تنوعت زوايا التناول التي ركّزت عليها تفاعلات المستخدمين السعوديين حول قضية الخصوصية والأمن السيبراني، فجاءت نسب ظهورها كما يلي:

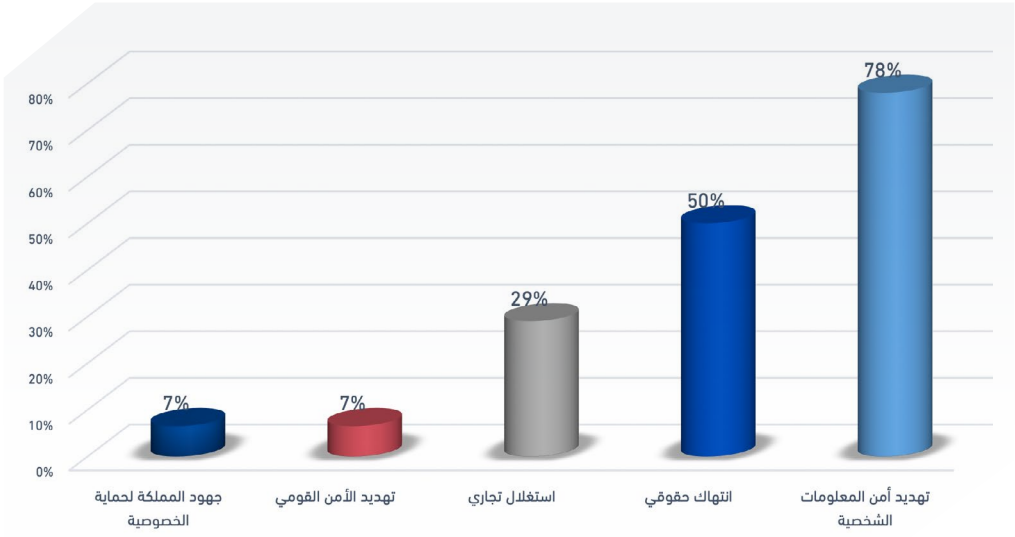
- **تهديد أمن المعلومات الشخصية:** استخدمت هذه الفئة من التفاعلات لغة تحذيرية وتوعوية ركّزت على توجيه المستخدمين بعدم استعراض خصوصياتهم على وسائل التواصل الاجتماعي، وأيضًا إرشادهم بالمخاطر التي قد تنتج عن استخدام بعض تطبيقات المتجر على الهواتف الذكية، مستشهدة بتوصيات المتخصصين في مجال الأمن السيبراني بضرورة وأهمية التوقف عن استخدام بعض التطبيقات، بل وحذفها لأسباب تتعلق بانتهاك خصوصياتهم وأمنهم ومنها الوصول إلى معلوماتهم الشخصية وجهات الاتصال ومعرفة الأماكن التي يقصدونها، وذلك دون وجود موافقة مسبقة تسمح للتطبيق بمعرفة هذه البيانات.

- **انتهاك حقوقي:** وفيه تم التركيز على أن بيانات المستخدمين هي جزء أصيل من خصوصيتهم، ولا يحق لشركات المنصات الاجتماعية انتهاكها أو استخدامها بأي شكل دون موافقة أصحابها.

- **استغلال تجاري:** تناولت هذه الفئة قضية الخصوصية والأمن السيبراني من منظور استغلال التطبيقات ومنصات التواصل الاجتماعي لبيانات المستخدمين واستخدامها كسلعة يتم بيعها للشركات والمعلنين بهدف تحقيق الربح المادي.

- **تهديد الأمن القومي:** ذهبت فئة من التفاعلات إلى تناول انتهاك الخصوصية من منظور أعم وأشمل يتعلق بتهديد أمن واستقرار الدول، فاستعرضت تجارب بعض الحكومات التي اتخذت إجراءات قانونية لحماية الخصوصية، كما قامت بحظر التطبيقات والبرامج والمنصات التي تنتهك الخصوصية، واهتمت هذه الفئة من التفاعلات أيضًا بتناول القضية من منظور الحروب السيبرانية بين الدول كشكل جديد من أشكال الصراعات الدولية.

- **جهود المملكة لحماية الخصوصية:** حرصت هذه الفئة على إبراز وتثمين الدور الذي تقوم به المملكة العربية السعودية لتوفير أكبر قدر من الحماية لخصوصية مؤسساتها ومواطنيها، وسعيها الدائم لامتلاك أفضل التقنيات في مجال الأمن السيبراني من أجل مواجهة كافة أنواع الاختراقات والتهديدات السيبرانية، فضلًا عن تبني الدولة السعودية سياسة قائمة على تثقيف وتوعية المواطنين بشأن ضرورة الحفاظ على خصوصية المعلومات، وتحذيرهم من الانتهاكات التي تُهدد خصوصيتهم.



أنماط التناول

أظهرت نتائج الدراسة أن تناول المستخدمين السعوديين لقضية الخصوصية والأمن السيبراني انقسم إلى نمطين رئيسيين، هما:

- **تناول تفصيلي:** حلّ في المرتبة الأولى بنسبة 53%، وفيه قام المستخدمون بتقديم نصائحهم وإرشاداتهم حول كيفية ضبط إعدادات الخصوصية للمواقع الإلكترونية والمنصات الاجتماعية وتطبيقات المتجر على الهواتف الذكية لمنع التسلل واختراق خصوصية بياناتهم الشخصية أو الوصول إلى ملفات الصور والفيديوهات الخاصة بهم، أو تتبُّع موقعهم الجغرافي، أو التعرف على ميولهم وتفضيلاتهم دون الحصول على موافقتهم المُسبقة كمستخدمين.

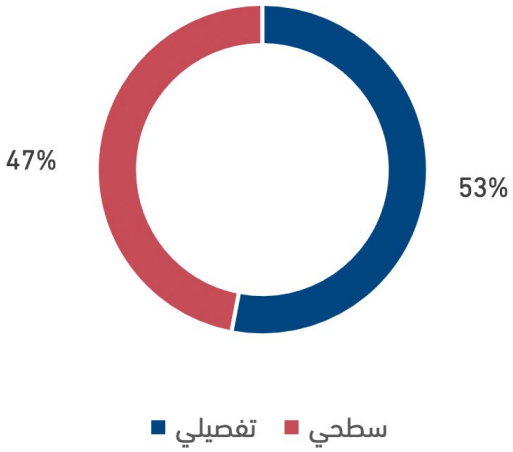
كما جاء تناول هذه الفئة مصحوبًا بتحذيرات تتعلق بمخاطر انتهاك الخصوصية، سواء كانت هذه المخاطر تتعلق بالشخص أو مكان العمل أو الوطن، فضلًا عن استعراضهم للأساليب التي تتبعها شركات التكنولوجيا من أجل استغلال بيانات المستخدمين لأغراض تجارية والتربح من ورائها.

وشدّدت بعض تفاعلات هذه الفئة على أهمية عدم إفراط الأشخاص في استخدام وسائل التواصل الاجتماعي؛ لأنها تُمثل تهديدًا حقيقيًّا للخصوصية، وطالبت بضرورة إقرار القوانين والتشريعات الكفيلة بتوفير أقصى درجات الحماية لأمن وخصوصية بيانات المستخدمين، مستشهدة في ذلك بتجارب عدد من الدول.

وكان من اللافت أن تفاعلات هذه الفئة استشهدت بالرسائل الاتصالية الصادرة عن حسابات الجهات الحكومية المعنية بمجال الأمن السيبراني مثل الهيئة الوطنية للأمن السيبراني، كما استشهدت أيضًا بالمواد المنشورة في وسائل الإعلام السعودية وعلى رأسها مقالات الرأي، وذلك كنوع من التوثيق والتأكيد والبرهنة على صحة طرحها؛ مما يُبرهن على الدور المؤثر الذي تقوم به الجهات الحكومية ووسائل الإعلام في تشكيل اتجاهات ومعارف المواطنين حول قضية الخصوصية والأمن السيبراني.

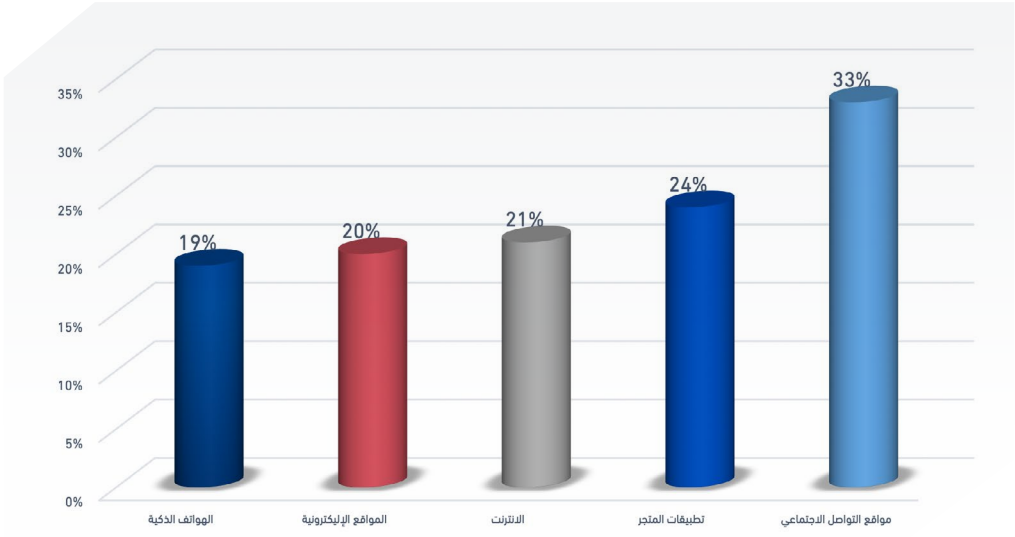
وتعكس هذه النتيجة مؤشرًا مهمًا يتمثل في أن أكثر من نصف عينة الدراسة لديهم قدر كبير من المعرفة حول التحديات والتهديدات السيبرانية التي تواجه المملكة ومؤسساتها ومواطنيها.

- **تناول سطحي:** جاء في المرتبة الثانية بنسبة 47%، وقد اتسمت تفاعلات هذه الفئة بالعمومية في الطرح دون التطرق إلى التفاصيل أو الشرح والتفنيد، ومن أمثلة ذلك التحذير من إمكانية اختراق وانتهاك الخصوصية ولكن دون عرض الكيفية التي يتم بها هذا الاختراق أو كيفية تفاديه وتجنبه.



مصادر تهديد الخصوصية وأمن المعلومات

تضمنت تفاعلات المستخدمين السعوديين محل الدراسة مجموعة من المصادر التي تُشكل – حسب رؤيتهم – تهديدًا للخصوصية وأمن المعلومات، فظهرت مواقع التواصل الاجتماعي في المرتبة الأولى بنسبة 33%، تلاها تطبيقات المتجر في المرتبة الثانية بنسبة ظهور بلغت 24%، ثم الإنترنت في المرتبة الثالثة بنسبة ظهور 21%، وظهرت المواقع الإلكترونية بالمرتبة الرابعة بنسبة 20%، أما الهواتف المحمولة فحصلت على المرتبة الخامسة والأخيرة بنسبة ظهور بلغت 19%.



وتكشف هذه النتيجة وجود اتفاق بين المستخدمين وكُتّاب الرأي السعوديين حول أن مواقع التواصل الاجتماعي تُمثل مصدر التهديد الأول للخصوصية وأمن المعلومات. كما يوجد توافق حول المصادر الأخرى المُهددة وإن اختلفت نسبتها وفق منظور كل طرف.

اتجاهات المستخدمين نحو الخصوصية

انتهت نتائج تحليل عينة الدراسة إلى عدم وجود أي اتجاه داعم أو مؤيد لـ «الحرية المطلقة» في استخدام الإنترنت ووسائل التواصل الاجتماعي، بل على العكس، أظهرت جميع تفاعلات المستخدمين إدراكهم لأهمية الخصوصية ومخاطر انتهاكها أو اختراقها، إلا أن الاختلاف كان في مدى التزامهم بتطبيق الإجراءات الكفيلة بالحفاظ على أمن وخصوصية بياناتهم الشخصية؛ حيث عبّرت الغالبية العظمى من التفاعلات عن الالتزام بتطبيق هذه الإجراءات سواء من خلال التدابير الذاتية للمستخدم، أو بواسطة الإجراءات والضوابط التي تتخذها مؤسسات الدولة، وبالتالي كانوا مؤيدين لفكرة «الحرية المنضبطة»، ومثّل هذا الاتجاه 97.5% من إجمالي التفاعلات، ومن الاستشهادات على ذلك ما يلي:

- جزء من المسؤولية يقع على الأفراد أنفسهم في حماية خصوصيتهم من خلال عدم نشر صور أو بيانات شخصية أو عرض حياتهم الخاصة على المشاع.
- شرح كيفية تفعيل إعدادات الخصوصية على منصات التواصل الاجتماعي.
- التنبيه بضرورة قراءة سياسة الخصوصية قبل الشروع في الاشتراك أو التسجيل في أي تطبيق أو منصة.
- التأكيد على أهمية تثقيف الأبناء وتوعيتهم بمخاطر الاستخدام العشوائي للمنصات الاجتماعية والتطبيقات الإلكترونية.
- التشديد على أهمية دور الدولة في حماية خصوصية الأفراد، وذلك عبر فرض قوانين منظمة للخصوصية عبر الانترنت.
- مطالبة الدولة بالتدخل من أجل الضغط على شركات التكنولوجيا وإجبارها على الالتزام بالمواثيق والأخلاقيات التي تحفظ الخصوصية، لأن انتهاكها يُشكّل تهديدًا للأمن الشخصي والقومي.

أما النسبة المتبقية من التفاعلات والتي تبلغ 2.5%، فعلى الرغم من أن محتوى تغريداتها عكس إدراكها لأهمية الخصوصية والحفاظ على أمن المعلومات، إلا أنها أظهرت نوعًا من التهاون في الالتزام بتطبيق الإجراءات الكفيلة بالحفاظ عليها، ومن أمثلة ذلك تغريدة تقول: «على الرغم من تحذيري الدائم من مخاطر انتهاك الخصوصية، فإنني في الوقت نفسه أكتب على تويتر دون تحفظ بشأن معلوماتي الشخصية، هذا تناقض».

وقد تكرر هذا «السلوك المتناقض مع القناعات» لأسباب مختلفة كالتهاون، أو الكسل بسبب الطول النسبي – ربما المقصود – لبنود وسياسات الخصوصية للشركات المختلفة، أو بسبب غلبة دافع «الرغبة في الظهور والانتشار» على دافع «حماية المعلومات الشخصية».

الالتزام بالتطبيق

%97.5

عدم الالتزام

%2.5

النتائج العامة للدراسة

انتهت الدراسة إلى مجموعة من النتائج، أهمها:

- وجود توافق بين المضامين المقدمة في مقالات كُتّاب الرأي وحساب الهيئة الوطنية للأمن السيبراني على تويتر.

- انعكست كل من معالجة كُتّاب الرأي في الصحف السعودية والرسائل الاتصالية المتضمنة في حساب الهيئة الوطنية للأمن السيبراني بتويتر إيجابًيا على إدراك المستخدمين لأهمية الأمن السيبراني وضرورة الحفاظ على حماية الخصوصية.

- أكدت الأطروحات المقدمة من كُتّاب الرأي وحساب الهيئة وأيضًا المستخدمين على الدور المتميز والمهم والحيوي الذي تقوم به المملكة بقيادة خادم الحرمين الشريفين الملك سلمان بن عبد العزيز وجهود صاحب السمو الملكي الأمير محمد بن سلمان ولي العهد – حفظهما الله – في تعزيز منظومة الأمن السيبراني، وتوفير أقصى درجات الحماية والأمان للمواطنين ومؤسسات الدولة، وفق أفضل التقنيات العالمية الحديثة.

- أسفرت الجهود المضنية التي تقوم بها الدولة السعودية وبتوجيهات من القيادة الرشيدة صاحبة الرؤى الثاقبة عن تحقيق المملكة طفرة نوعية مذهلة في وقت قياسي في مجال الأمن السيبراني.

- اتفق كل من كُتّاب الرأي والمستخدمين على أن مواقع التواصل الاجتماعي تُمثل مصدر التهديد الأول للخصوصية وأمن المعلومات. كما يوجد توافق حول المصادر الأخرى المُهددة وإن اختلفت نسبتها وفق منظور كل طرف.

توصيات الدراسة

إجمالًا.. إن سياسات المملكة العربية السعودية المتعلقة بالتحول الرقمي وفق مستهدفات رؤية السعودية 2030 تسير بخطى ثابتة في مجالات الأمن السيبراني، حيث تعمل الدولة بشكل متوازٍ على عدة محاور، منها:

- تعزيز قدرات المملكة في مجال الأمن السيبراني لمواجهة كافة أنواع التحديات والمخاطر.

- تثقيف وتوعية المواطنين بهذا المجال الحيوي وخطورته وكيفية الوقاية من تهديداته.

- قيام مؤسسات الدولة بدور متميز في حماية المواطنين والمنشآت الحكومية والخاصة.

- بناء وتأهيل القدرات الوطنية المتخصصة في مجال الأمن السيبراني بحيث تكون هناك كوادر سعودية مؤهلة علميًّا وعمليًّا وفق أحدث النظم المعمول بها عالميًّا.

وانطلاقًا من نتائج الدراسة، يُوصي مركز القرار بما يلي:

- أهمية تعزيز دور وسائل الإعلام المختلفة ونخب المجتمع لمساعدة المؤسسات الحكومية في تثقيف وتوعية المواطنين بمخاطر التهديدات السيبرانية، وضرورة الحفاظ على الخصوصية.
- الوضع في الاعتبار أنه كلما زاد الاعتماد على التقنيات الحديثة ارتفعت معدلات الاستهداف السيبرانية، ولذلك فمن الأهمية بمكان التشديد المستمر على اتباع الأفراد والمؤسسات لإرشادات الأمان وحماية الخصوصية.
- تكثيف الحملات الإعلامية التي تُحذر من مخاطر التهاون مع خصوصية المعلومات الشخصية، وعرض هذه الحملات في وسائل الإعلام التقليدي والجديد، وبشكل خاص وسائل التواصل الاجتماعي.
- يجب أن تُؤكد الرسائل الاتصالية الصادرة عن الجهات الحكومية والمؤسسات الإعلامية على ما يلي:
  - أن الدور المؤسسي والحكومي لا يكفي وحده لتوفير الحماية، فلا بد من تفعيل الرقابة الذاتية للأفراد واتخاذهم لكافة الإجراءات الاحترازية للحفاظ على خصوصياتهم.
  - الحفاظ على خصوصية المعلومات الشخصية لا يحمي الفرد فقط، ولكن يُمثل حماية للأمن القومي للبلاد.

مركـز القرار
للدراسات الإعلامية

..نـخـطـو
بـقـرارك

تابع حسابنا على تويتر

www.alqarar.sa

@alqarar_sa