



دراسات المستقبل

سلسلة دراسات تصدر شهرياً عن المستقبل للأبحاث والدراسات المتقدمة أبوظبي، الإمارات العربية المتحدة



The End of Privacy

ملامح الخصوصية والانكشاف في عصر التقنيات الذكية

د. فاطمة الزهراء عبدالفتاح

تقديم: إيهاب خليفة

العدد 7 - سبتمبر 2019

سعر النسخة: الإمارات 16 درهم | الكويت 1 دينار | البحرين 1.5 دينار | عُمان 1.5 ريال | الأردن 2 دينار | لبنان 5000 ليرة | مصر 10 جنيهات | تونس 4 دنانير | المغرب 20 درهم



دراسات المستقبل

المدير الأكاديمي:

د. محمد عبدالسلام

نائب المدير:

أ. إبراهيم غالي
أ. حسام إبراهيم

رئيس التحرير التنفيذي:

أحمد عثمان

نائب رئيس التحرير:

د. شادي عبدالوهاب

هيئة التحرير:

علي صلاح
أحمد عاطف
إيهاب خليفة
هالة الحفناوي
مصطفى ربيع
إبراهيم الغيطاني
بسمة الإتربي
يارا منصور
منى مصطفى
عبد اللطيف حجازي

الإخراج الفني:

عبدالله خميس

العلاقات العامة:

رحاب مكرم

info@futureuae.com

عن "دراسات المستقبل"

سلسلة دراسات أكاديمية، تصدر شهرياً عن "المستقبل للأبحاث والدراسات المتقدمة"، وتركز كل دراسة على قضية واحدة، تمثل ظاهرة صاعدة على المستوى الاستراتيجي، تتسم بالتعقيد وتعدد الأبعاد، وتهيمن على الجدول العام في الشرق الأوسط والعالم.

وتتناول "السلسلة" الاتجاهات والتحولات الرئيسية في المجالات الأمنية والسياسية والاقتصادية والاجتماعية والتكنولوجية، والظواهر كافة التي يمكن أن تساهم في تشكيل مستقبل الشرق الأوسط.

*الآراء الواردة في الإصدار تعبر عن كتابها، ولا تعبر بالضرورة عن "دراسات المستقبل" أو آراء مركز المستقبل للأبحاث والدراسات المتقدمة.



مركز المستقبل:

مركز تفكير (Think Tank) مستقل، أنشئ عام 2014، في أبوظبي، بدولة الإمارات العربية المتحدة، للمساهمة في تعميق الحوار العام، ومساندة صنع القرار، ودعم البحث العلمي، فيما يتعلق باتجاهات المستقبل، التي أصبحت تمثل إشكالية حقيقية بالمنطقة، في ظل حالة عدم الاستقرار وعدم القدرة على التنبؤ، خلال المرحلة الحالية، من خلال رصد وتحليل وتقدير «المتغيرات» المتعلقة بالتحويلات السياسية والاتجاهات الأمنية، والتوجهات الاقتصادية والتطورات التكنولوجية، والتفاعلات المجتمعية والثقافية، المؤثرة على مستقبل منطقة الخليج، وفي نطاق الشرق الأوسط عموماً.

سياسة النشر:

تعتمد سياسة النشر في دراسات المستقبل على التكليف المباشر للكتاب والمتخصصين، ويمكن قبول مقترحات الباحثين والمحللين من دول المنطقة والعالم، لإعداد موضوعات للنشر في الدورية، عبر الإرسال أو الاتصال بمسؤول التحرير.

لا يجوز استنساخ أي جزء من هذه الدراسة أو نقلها بأي شكل أو وسيلة، سواء أكانت إلكترونية أم ميكانيكية، بما في ذلك النسخ الضوئي أو التسجيل أو أي نظام لتخزين المعلومات أو استعادتها، دون الحصول على إذن كتابي مسبق من مالك حقوق النشر، يرجى توجيه جميع الاستفسارات إلى الناشر، الدورية، عبر الإرسال أو الاتصال بمسؤول التحرير.
info@futurecenter.ae

وكلاء التوزيع في الخارج:

عمان: مؤسسة العطاء للتوزيع، هاتف: 0096824491399
البحرين: الهلال للخدمات المباشرة والتوزيع، هاتف: 0097317290000
الكويت: شركة مجموعة النظائر الاعلامية، هاتف: 0096524746500
لبنان: مؤسسة نعنوع الصحفية، هاتف: 009611666668
الأردن: وكالة التوزيع الأردنية، هاتف: 009625358855
مصر: مؤسسة الأهرام، هاتف: 0020227704213
تونس: الشركة التونسية للصحافة، هاتف: 0021671322499
المغرب: شركة سوشبريس، هاتف: 00212522589931

للاتصال والمعلومات:

البرج الدولي، شارع الكرامة، منطقة مركز المعارض، الطابق (24)
ص.ب 111414 أبوظبي، الإمارات العربية المتحدة
هاتف: +971-24444513، فاكس: +971-24444732
العلاقات العامة: 473 480 544 971+
Email: info@futureuae.com
www.futureuae.com

منافذ التوزيع:

يتم التوزيع داخل دولة الإمارات العربية المتحدة بواسطة "شركة أبوظبي للإعلام"، ص.ب: 40401 - أبوظبي.

الاشتراكات:

للاشتراك من داخل الدولة اتصل بالرقم المجاني:

800 2220

أو راسلنا عبر عنوان البريد الإلكتروني:

subscriptions@admedia.ae



مقدمة المحرر

في بداية انتشار الإنترنت في التسعينيات من القرن الماضي وبداية الألفية الثانية ظهرت بعض القوانين والتشريعات التي تحمي بيانات الأفراد المستخدمة عبر الإنترنت، وقد اتسمت بيانات الأفراد في هذه الفترة بكونها محدودة وقليلة للغاية وتقتصر على الاسم والصورة ورقم الهاتف، لكن مع التطورات التكنولوجية المستمرة وزيادة اعتماد الأفراد على الإنترنت والتقنيات الذكية المختلفة في حياتهم اليومية كالهواتف الذكية وأجهزة إنترنت الأشياء والمساعدات الشخصية والأجهزة التي تعمل بالأوامر الصوتية، زاد حجم ونوع البيانات الشخصية التي يمكن الحصول عليها عبر الإنترنت.

وتمتد هذه البيانات لتشمل بيانات الأفراد الحيوية، مثل بصمة العين والوجه واليد والبصمة الوراثية (DNA)، فضلاً عن البيانات الصحية كالطول والوزن ومعدل ضربات القلب ونسبة السكر في الدم ومعدل الحركة اليومية ونسبة حرق الدهون والحالة المرضية للمستخدم بصورة عامة، هذا خلافاً عن الموقع الجغرافي الحالي ومكان العمل والإقامة وأي أماكن أخرى يتردد عليها، والعديد من المعلومات الشخصية الأخرى، مثل نوعية الأطعمة والمشروبات والملابس والأفلام والكتب والموسيقى التي يفضلها المستخدم وسجل مشترياته كاملاً عبر الإنترنت، ومواعيد عمله ونومه وغذائه، وتحديد شبكة أصدقائه وأفراد عائلته، وإن أردت الإيجاز فقل إن الأجهزة الذكية تعلم عن الإنسان أكثر مما يعلم هو عن نفسه.

وتكمن الخطورة في أن البيانات هي أساس العالم الرقمي الحالي، وجمعها ضروري للشركات بهدف تحسين الخدمات التي تقدمها لعملائها، سواء خدمات البحث عن التفضيلات أو خدمة الإعلانات أو ترشيحات الأخبار والكتب والأفلام وخلافه، فضلاً عن كونها البنية الأساسية لتطوير نظم الذكاء الاصطناعي وتعلم الآلات والسيارات ذاتية القيادة وغيرها، فهي تحتاج كميات كبيرة من البيانات العملاقة لكي تتعلم القيام بوظائفها، فالبيانات هي أساس عملية التطور التكنولوجي وهي الوحدة لبناء الثورة الصناعية الرابعة.

إلا أن عملية الحفاظ على هذه البيانات من إساءة الاستخدام هو التحدي الرئيسي الذي يواجه المستخدمين كافة للأجهزة الذكية، سواء الحفاظ عليها من الاختراق والقرصنة وإساءة استخدامها من قبل المجرمين الذي يستطيعون سرقة البيانات الحيوية للأفراد من الأجهزة الذكية وانتحال شخصياتهم الحقيقية في القيام بأعمال إجرامية، أو الحفاظ عليها من إساءة استخدام شركات التكنولوجيا لهذه المعلومات لتحقيق مكاسب مالية أو سياسية على حساب خصوصية المستخدمين.

ويتضح الاستغلال المالي لهذه البيانات في تحقيق عوائد مالية من الإعلانات التي تقدمها هذه الشركات، أو في تطوير منتجات ذكية استهلاكية لاستمرار تحقيق الريادة في سوق الأجهزة الذكية، وهو ما يدفع للتساؤل عن حق المستخدم في هذه العوائد والمكاسب المالية العملاقة، وذلك بافتراض أن الأفراد موافقون على استخدام بياناتهم من الأساس، ولماذا لا يحصلون على الأجهزة الذكية والمساعدات الصوتية الشخصية، مثل "مساعد جوجل" (Google Assistant) أو إيكسا التابعة لأمazon بالمجان، فهذه الأجهزة تقوم مثلاً بإجراء حجوزات لدى العديد من الجهات لصالح الأفراد كموعده عند الطبيب أو الحلاق أو في السينما، وهؤلاء يدفعون لجوجل لكي تقدمهم في ترشيحات الإعلانات عبر الإنترنت أو عبر المساعد الشخصي، وتحقق جوجل منفردة العوائد الكبيرة، من دون النظر إلى حق الأفراد في الاستفادة من بياناتهم الشخصية.

ويتضح الاستغلال السياسي للبيانات فيما كشفت عنه فضيحة شركة كامبريدج أناليتيكا، حيث عمدت هذه الشركة إلى استخدام بيانات الأفراد الشخصية على موقع الفيس بوك ودراسة اهتماماتهم وتوجهاتهم في التأثير على العملية الديمقراطية وتغيير توجهات الناخبين، سواء كان

ذلك عبر الاستفتاء في بريطانيا على الخروج من الاتحاد الأوروبي أو أثناء الانتخابات الرئاسية الأمريكية عام 2016.

ومن الأمثلة على التوظيف السياسي للبيانات قيام العديد من المتظاهرين في هونج كونج والمعترضين على اعتزام الحكومة إقرار مشروع قانون يسمح لسلطات الإقليم بتسليم المشتبه بهم والمطلوبين إلي الصين لمحاكمتهم هناك، بتحطيم كاميرات المراقبة والتعرف على الوجوه هناك، أو ارتداء اقنعة أو استخدام مظلات شخصية تمنع الكاميرات من التعرف على هؤلاء الأفراد خشية ملاحقتهم من قبل السلطات.

وقد اتجهت العديد من دول العالم مؤخراً لإصدار قوانين تنظم عملية استخدام وتداول وحفظ هذه البيانات، فأصدر الاتحاد الأوروبي "اللائحة العامة لحماية البيانات" المعروفة اختصاراً بـ (GDPR) في نهاية مايو عام 2018، وفي يوليو 2018 أقرت ولاية كاليفورنيا قانوناً لحماية بيانات الأفراد، بما يمهّد لموجة تشريعية تمثل بداية حقيقية لتقييد حرية الشركات في إساءة استخدام بيانات المستخدمين.

وقد حان الوقت للحديث عن حق الإنسان في الحصول على البيانات الشخصية من هذه الشركات، والحق أيضاً في النسيان (The Right To Be Forgotten) أي أن يتم محو السجل الشخصي الرقمي كاملاً، وكذلك الحق في المشاركة في الربح والعائد المادي الناجم عن الانتفاع بهذه البيانات.

ومن هنا، تحاول هذه الدراسة إلقاء الضوء على المفهوم الواسع لاختراق الخصوصية أو الانكشاف السيبراني، وقد رسمت الدراسة ملامح وخصائص هذا المجتمع في عدة أركان رئيسية منها تطور تقنيات جمع المعلومات وظهور أنواع جديدة من المعلومات وانتشار تحليل البيانات الضخمة وتقنيات تمييز الهويات الشخصية وظهور الجدل حول ملكية البيانات والوعي بمفاهيم استغلالها.

كما حللت أيضاً التغيرات الجوهرية التي طرأت على خصوصية الأفراد وجعلتها أكثر انكشافاً وعرضة لإساءة الاستغلال، والتي حددتها الدراسة في انتشار الهواتف الذكية، ووسائل التواصل الاجتماعي، وتطبيقات الطرف الثالث، وتقنيات الذكاء الاصطناعي، وإتترنت الأشياء، والحوسبة السحابية والحوسبة الكمية، وبرمجيات القرصنة والاختراق، والشركات المزودة لخدمات الإنترنت.

وفي النهاية حاولت الدراسة أن تستعرض اتجاهات مقاومة الانكشاف السيبراني واختراق الخصوصية، وذلك عبر أربع طرق رئيسية تقنية، وتشريعية، وحكومية، ودولية، تتمثل في تطوير تقنيات تساعد في حماية الخصوصية الشخصية أو عبر الطرق والأساليب القانونية والتشريعية أو من خلال تطبيق مفهوم حوكمة البيانات (Data Governance) الذي يعنى بوضع نظام لعمليات صناعة القرار والمحاسبة للعمليات القائمة على المعلومات.

ولقد قامت بإعداد هذه الدراسة د.فاطمة الزهراء عبدالفتاح، مدرس الصحافة وتكنولوجيا الاتصال بكلية الإعلام جامعة الأهرام الكندية، حيث حصلت على درجتي الماجستير والدكتوراه من جامعة القاهرة، ولها أكثر من عشرين كتاباً وورقة بحثية في مجال التكنولوجيا والإعلام الرقمي وتأثيراتهما السياسية والأمنية والاجتماعية. وعلى مدار عشر سنوات، أسست وأدارت مركز المصري لدراسات والمعلومات، كما عملت مديراً لتحرير مجلة "شؤون خليجية" العلمية المحكمة، فضلاً عن تقديمها استشارات بحثية وتدريبية للعديد من المؤسسات الدولية والعربية، مثل منظمة الأمم المتحدة للتربية والعلوم والثقافة (اليونسكو) وجامعة الدول العربية ومؤسسة الصوت الحر الهولندية والجامعة الأمريكية بالقاهرة.

أ.إيهاب خليفة

رئيس وحدة التطورات التكنولوجية - المستقبل للبحوث والدراسات المتقدمة، أبوظبي

المحتويات:

6	مقدمة الدراسة
6	أولاً: أركان وخصائص "الانكشاف المعلوماتي"
7	1- اتساع حجم السوق الرقمية:
7	2- تطور تقنيات جمع المعلومات:
7	3- ظهور أنواع جديدة من البيانات:
8	4- انتشار تحليل البيانات الضخمة:
9	5- تمييز الهوية الشخصية:
10	6- الجدل حول ملكية البيانات:
10	7- الموافقة على جمع البيانات:
11	8- الوعي بمفاهيم استغلال البيانات:
11	ثانياً: مداخل اختراق الخصوصية في بيئة المعلومات
11	1- الهواتف الذكية:
13	2- وسائل التواصل الاجتماعي:
15	3- تطبيقات الطرف الثالث:
16	4- تقنيات الذكاء الاصطناعي:
17	5- إنترنت الأشياء:
19	6- الحوسبة السحابية والحوسبة الكمية:
20	7- برمجيات القرصنة والاختراق:
23	8- الشركات المزودة لخدمة الإنترنت:
23	ثالثاً: آليات مواجهة تهديدات الخصوصية
23	1- المقاومة التقنية:
24	2- المقاومة التشريعية:
27	3- حوكمة البيانات:
28	4- التضامن الدولي:
28	خاتمة الدراسة