



تطبيق Waze بين الملاحاة الرقمية والأمن القومي العراقي

بقلم

بختيار أحمد صالح

باحث في مركز حمورابي للبحوث والدراسات الاستراتيجية



تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزاً علمياً بحثياً يهتم بدراسة الموضوعات السياسية والاجتماعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

- لا يجوز إعادة نشر أي من هذه الأوراق البحثية إلا بموافقة المركز، وبالإمكان الاقتباس بشرط ذكر المصدر كاملاً.
- لا تعبر الآراء الواردة في الورقة البحثية عن الاتجاهات التي يتبناها المركز وإنما تعبر عن رأي كاتبها.
- حقوق الطبع والنشر محفوظة لمركز حمورابي للبحوث والدراسات الاستراتيجية.

للتواصل

مركز حمورابي

للبحوث والدراسات الاستراتيجية

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net



مقدمة

أصبحت تطبيقات الملاحة الرقمية جزءاً من البنية اليومية للحياة الحضرية، لكنها لم تعد مجرد أدوات لتحديد الاتجاهات؛ إذ تعتمد بعض خدماتها على بيانات الموقع الجغرافي، وسجل الرحلات، ومعلومات حركة المرور التي يساهم المستخدمون في إنتاجها. ويشير ذلك أسئلة تتعلق بخصوصية الأفراد، وحماية البيانات الحساسة، وإمكان الاستفادة من المعلومات المكانية في التحليل الأمني.

تكتسب هذه القضية أهمية خاصة في العراق، بالنظر إلى حساسية البيئة الأمنية في بغداد، ووجود مؤسسات حكومية وعسكرية ومنشآت دبلوماسية ومناطق ذات قيود على الدخول والحركة.

وتتناول هذه الورقة تطبيق Waze من خلال ثلاثة محاور مترابطة: خلفية تأسيسه وعلاقة بعض مؤسسيه بوحدة الاستخبارات العسكرية "الإسرائيلية" 8200؛ وطبيعة البيانات التي يجمعها التطبيق وفق سياساته المعلنة؛ ثم تقييم المخاطر المحتملة المرتبطة باستخدامه في العراق، مع التمييز بين المخاطر التقنية القابلة للتحليل والادعاءات التي لا تتوافر بشأنها أدلة كافية.

وتؤكد سياسة الخصوصية المنشورة للتطبيق أن بيانات الموقع والرحلات وسجل الملاحة تدخل ضمن المعلومات التي يمكن جمعها، مع اختلاف نطاق الجمع بحسب إعدادات الجهاز والحساب والخدمات المستخدمة.

وتتمثل الفرضية الأساسية للورقة في أن مصدر القلق الأمني الأكثر قابلية للتحقق ليس الخلفية العسكرية لمؤسسي التطبيق وحدها، بل طبيعة البيانات المكانية التي ينتجها المستخدمون، ومدى حمايتها، وإمكان ربطها بمصادر أخرى، ومدى خضوع استخدامها للرقابة القانونية والمؤسسية.

أولاً: وحدة 8200 والعلاقة بين الاستخبارات والاقتصاد التكنولوجي "الإسرائيلي"

1. طبيعة وحدة 8200

تُعد وحدة 8200 إحدى أبرز وحدات الاستخبارات العسكرية "الإسرائيلية"، وترتبط بصورة أساسية باستخبارات الإشارات وجمع المعلومات الإلكترونية وتحليلها، إلى جانب قدرات تقنية متقدمة في مجالات الاتصالات والحوسبة والأمن السيبراني. وتشير المعلومات إلى أن تأثير الوحدة يتجاوز مهامها العسكرية؛ إذ أسهمت خبرات أفرادها وشبكاتهم المهنية في نشوء شركات تكنولوجية وأمنية "إسرائيلية". كما أن للثقافة التنظيمية، والموارد البشرية، وتراكم الخبرة التقنية، والعلاقات مع القطاع الخاص، عوامل أساسية في تفسير هذا التأثير.

ولا يعني ذلك أن جميع الشركات التي أسسها أفراد خدموا في الوحدة تعمل لصالح المؤسسة العسكرية، أو أن منتجاتها المدنية مصممة لأغراض استخباراتية. وإنما يوضح وجود مسار لنقل الخبرة والمهارات من المؤسسة العسكرية إلى القطاع التجاري، وهو مسار يمكن دراسته من منظور الاقتصاد السياسي للتكنولوجيا والأمن القومي.

2. أوري ليفين وتأسيس Waze

تُظهر السيرة المهنية المنشورة لأوري ليفين أنه أحد مؤسسي Waze عام 2007، وأنه خدم في وحدة 8200 مطوراً للبرمجيات قبل انتقاله إلى عالم ريادة الأعمال. وقد استحوذت Google على Waze عام 2013 في صفقة بلغت قيمتها المعلنة نحو 1.1 مليار دولار. وتكشف هذه الوقائع عن تقاطع بين خبرة مؤسس التطبيق في بيئة تقنية عسكرية وبين تأسيس شركة مدنية تعتمد على البرمجيات والبيانات المكانية.

3. القيمة الاستراتيجية للعلاقة بين المؤسسة العسكرية والقطاع الخاص

توضح تجربة وحدة 8200 كيف يمكن للمعرفة المتراكمة في مجالات البرمجيات وتحليل البيانات والاتصالات أن تنتقل إلى القطاع التجاري. وهذه الظاهرة ليست محصورة بـ"إسرائيل"؛ إذ تشهد دول أخرى انتقالاً للخبرات بين المؤسسات الدفاعية وشركات التكنولوجيا والأمن السيبراني. وتبرز أهمية هذه العلاقة عندما تكون التقنيات التجارية قادرة على إنتاج بيانات واسعة النطاق أو تحليلها. فالقيمة الاستراتيجية لا تنشأ بالضرورة من وجود وظيفة عسكرية مباشرة داخل المنتج، بل قد تنشأ من القدرة على معالجة المعلومات، أو تطوير أدوات تحليلية، أو الاستفادة من الخبرة البشرية المتخصصة.

ثانياً: ما البيانات التي يمكن أن يجمعها Waze؟

1. بيانات الموقع وسجل الرحلات

توضح سياسة الخصوصية الرسمية لـ Waze أن الخدمة قد تجمع معلومات تتعلق بموقع المستخدم وتنقلاته، وأن سجل الرحلات يمكن أن يتضمن معلومات عن الرحلات التي أُجريت أثناء استخدام التطبيق. كما تشير السياسة إلى أن نطاق جمع بيانات الموقع يتأثر بإعدادات الجهاز والحساب والخدمات المستخدمة. وتوضح إرشادات الخصوصية أن التطبيق قد يتحقق من الموقع حتى عندما لا يكون مستخدماً بصورة مباشرة، بحسب الإعدادات المفعلة، من أجل تقديم خدمات مثل التذكير بموعد الانطلاق المتوقع أو معلومات المرور. كما يستطيع المستخدم مراجعة سجل الملاحاة وحذف بعض بياناته المحفوظة، وفق الخيارات التي تتيحها الخدمة. وهنا يجب التمييز بين ثلاثة مستويات من المعلومات:

نوع البيانات	الاستخدام المدني المعتاد	الدلالة الأمنية المحتملة
الموقع الجغرافي	تحديد موقع المستخدم وتوجيهه	معرفة الموقع التقريبي أو الفعلي بحسب دقة البيانات
سجل الرحلات	تسهيل الملاحة واسترجاع الوجهات	استنتاج بعض أنماط التنقل المتكررة
بيانات حركة المرور	تحديد الازدحام والطرق البديلة	تحليل أنماط الحركة العامة في مناطق معينة
البلاغات التي يقدمها المستخدمون	الإبلاغ عن الحوادث والازدحام والمخاطر على الطريق	إنتاج معلومات آنية عن حالة الطرق، بحسب طبيعة البلاغات
معلومات الحساب والتفاعل	إدارة الخدمة وتخصيص بعض وظائفها	مخاطر إضافية إذا أمكن ربط البيانات بحساب أو شخص محدد

2. ماذا تكتسب البيانات المكانية؟

تكمن أهمية بيانات الموقع في أن دلالتها لا تقتصر على معرفة مكان المستخدم في لحظة معينة. فقد يصبح تكرار المعلومات عبر الزمن مفيداً لفهم بعض أنماط الحركة. وعلى المستوى العام، يمكن أن تساعد البيانات المكانية، عند توافرها بصورة قانونية ومناسبة، في دراسة حركة المرور، وتحديد المناطق التي تشهد ازدحاماً متكرراً، وتحسين التخطيط الحضري. أما من منظور الأمن الرقمي، فإن تراكم البيانات يثير أسئلة إضافية تتعلق بمدة الاحتفاظ بها، وإمكان ربطها بمعلومات أخرى، ومستوى إخفاء الهوية، واحتمال الوصول غير المصرح به إليها. وتتوقف درجة الخطر على عدة عوامل، منها دقة البيانات، ومدة الاحتفاظ بها، ومدى ارتباطها بحساب معروف، وإجراءات الحماية المتبعة، ونوع الجهات التي يمكنها الوصول إليها. المخاطر الحقيقية هنا لا تتطلب افتراض وجود مؤامرة استخباراتية؛ إذ يمكن أن تنشأ ببساطة من ضعف حماية البيانات، أو سوء إدارتها، أو إساءة استخدامها.

3. هل تعني سياسة الخصوصية أن كل البيانات متاحة دائماً؟

لا فوجود نص في سياسة الخصوصية يوضح أن التطبيق قد يجمع نوعاً معيناً من المعلومات لا يعني أن كل هذه البيانات تُجمع في كل الحالات، أو أنها محفوظة بصورة دائمة، أو أنها متاحة لجميع الجهات. كما أن وجود بيانات على خوادم الخدمة لا يعني أن جهة خارجية تستطيع الوصول إليها تلقائياً. لذلك، ينبغي أن يركز أي تقييم تقني على ما تجمعه الخدمة فعلياً في ظل إعدادات محددة، وكيف تعالج تلك البيانات، وما آليات الاحتفاظ والحذف، وما الضمانات المتعلقة بالوصول إليها ومشاركتها. وهذا يتطلب فحصاً مستقلاً، ولا يمكن حسمه بمجرد الاستناد إلى سياسة الخصوصية أو إلى خلفية أحد المؤسسين.

ثالثاً: Waze والأمن القومي العراقي

1. خصوصية البيئة الأمنية في بغداد

تضم بغداد مؤسسات حكومية ومقار دبلوماسية ومنشآت أمنية وعسكرية، فضلاً عن مناطق تخضع لإجراءات دخول خاصة. ولهذا، فإن إدارة المعلومات المكانية في هذه البيئة تستحق اهتماماً مؤسسياً، خصوصاً عندما يتعلق الأمر بأجهزة الموظفين الذين يتعاملون مع معلومات حساسة.

2. الفرق بين المعلومات الجغرافية العامة والمعلومات الحساسة

يمكن تقسيم المعلومات ذات الصلة بالأمن المكاني إلى ثلاث فئات:

أ. معلومات عامة: مثل الطرق الرئيسية والتقاطعات والمناطق الحضرية.

ب. معلومات تشغيلية: مثل أنماط الازدحام وأوقات الحركة، التي قد تتغير دلالتها بحسب السياق.

ج. معلومات أمنية محمية: مثل بيانات الدخول غير العامة، أو تفاصيل الانتشار الأمني، أو السجلات التي تربط هوية محددة بمهمة حساسة.

وتكمن مسؤولية المؤسسات العراقية في ضمان ألا تؤدي الممارسات الرقمية اليومية إلى كشف معلومات محمية، مع احترام حقوق المستخدمين وعدم تحويل الشكوك غير المثبتة إلى اتهامات.

رابعاً: التوصيات والسياسات المقترحة للعراق

1. إجراء تقييم وطني لمخاطر تطبيقات الملاحاة

- يوصى بأن تتولى الجهات العراقية المختصة، بالتعاون مع خبراء مستقلين في الأمن السيبراني وحماية البيانات، إعداد تقييم للتطبيقات التي تستخدم خدمات الموقع الجغرافي. وينبغي أن يتضمن التقييم:
- أ. مراجعة سياسات الخصوصية وشروط معالجة البيانات.
 - ب. تحديد أنواع المعلومات التي تطلب التطبيقات الوصول إليها.
 - ج. دراسة خيارات الاحتفاظ بالبيانات وحذفها.
 - د. تقييم مخاطر استخدام التطبيقات على الأجهزة الحكومية والرسمية.
 - هـ. التمييز بين المخاطر المثبتة والاحتمالات النظرية.

2. وضع سياسة خاصة بالأجهزة الحكومية

- من الضروري أن تعتمد المؤسسات الحكومية والأمنية سياسة مكتوبة تحدد التطبيقات المسموح باستخدامها على الأجهزة الرسمية، مع تصنيف الأجهزة بحسب مستوى حساسية المهام التي تؤديها. وتشمل السياسة المقترحة:
- أ. إخضاع التطبيقات المثبتة على الأجهزة الرسمية لمراجعة دورية.
 - ب. تقييد الوصول إلى الموقع والميكروفون وجهات الاتصال عندما لا تكون هذه الصلاحيات ضرورية.
 - ج. منع استخدام الأجهزة الشخصية في المهام التي تتطلب حماية معلومات حساسة، وفق ضوابط مؤسسية واضحة.
 - د. تدريب الموظفين على مخاطر مشاركة المعلومات المكانية والصور والبيانات الوصفية.
 - هـ. وضع إجراءات للتعامل مع الحوادث التي تنطوي على كشف بيانات أو وصول غير مصرح به.

3. تطوير إطار قانوني لحماية البيانات المكانية

تحتاج حماية البيانات إلى قواعد واضحة بشأن جمعها والاحتفاظ بها ومشاركتها ومعالجتها. وينبغي أن تحدد هذه القواعد حقوق المستخدمين، ومسؤوليات الشركات، وآليات الشكوى والمراجعة، والضمانات التي تحكم وصول الجهات العامة إلى البيانات. كما ينبغي أن تشمل حماية البيانات المكانية للأفراد، سواء أكانوا موظفين حكوميين أم مواطنين عاديين، مع توفير ضمانات رقابية تمنع إساءة استخدام المعلومات.

4. تعزيز السيادة الرقمية العراقية

- لا ينبغي أن ينحصر النقاش في قبول تطبيق أجنبي أو رفضه؛ فالقضية الأوسع هي قدرة العراق على إدارة بياناته وحماية بنيته الرقمية. ومن السياسات الممكنة في هذا المجال:
- أ. بناء معايير وطنية لتقييم مخاطر الخدمات الرقمية.
 - ب. رفع كفاءة المؤسسات المختصة في تحليل سياسات البيانات وتدقيق التطبيقات.
 - ج. دعم تطوير خدمات محلية للخرائط والملاحة، عندما تكون مجدية تقنياً واقتصادياً.
 - د. تحسين إدارة البيانات الحكومية وتصنيفها بحسب درجة حساسيتها.
 - هـ. تعزيز التعاون البحثي بين الجامعات والمؤسسات الحكومية وشركات الأمن السيبراني.
 - و. وضع معايير واضحة للتعامل مع مقدمي الخدمات الرقمية الأجانب، بما يشمل الشفافية والامتثال القانوني وحماية المعلومات.

الاستنتاجات الرئيسية

1. توجد صلة مهنية موثقة بين أوري ليفين، أحد مؤسسي Waze، ووحدة 8200 "الإسرائيلية". وتمثل هذه الصلة جزءاً من السياق الأوسع للعلاقة بين الخبرات العسكرية والتكنولوجيا التجارية في "إسرائيل".
2. يتيح Waze وظائف للملاحة تعتمد على بيانات الموقع والرحلات، وتقر سياسته المنشورة بجمع بعض هذه البيانات وفق إعدادات المستخدم وطبيعة الخدمة.
3. يمكن لبيانات الموقع أن تكتسب قيمة إضافية عندما تتراكم عبر الزمن أو تُربط بمعلومات أخرى.
4. ينبغي أن ينصب الاهتمام الأمني العراقي على تقييم البيانات والصلاحيات وآليات الحماية، وعلى وضع سياسات لاستخدام التطبيقات على الأجهزة الرسمية، بدلاً من الاكتفاء بخلفية المؤسسين.
5. لا تتحقق السيادة الرقمية من خلال رفض التكنولوجيا الأجنبية بصورة عامة، وإنما عبر القدرة على تقييمها والتحكم في استخدامها، وحماية البيانات، والتحقق من الادعاءات، ومساءلة الجهات التي تتعامل مع المعلومات الحساسة.

خاتمة

تكشف قضية Waze عن إشكالية أوسع من تطبيق واحد أو مؤسس واحد، ففي العصر الرقمي، قد تتحول البيانات التي ينتجها الاستخدام اليومي للتكنولوجيا إلى مورد ذي قيمة اقتصادية وأمنية. ويجعل هذا التحول حماية المعلومات المكانية جزءاً من مفهوم الأمن القومي الحديث. إن خلفية بعض مؤسسي التطبيق في وحدة 8200 تستحق أن تُدرس ضمن سياق العلاقة بين المؤسسة العسكرية "الإسرائيلية" والقطاع التكنولوجي والحماية المؤسسية الرشيدة تبدأ بفهم المعلومات التي تُجمع، وتحديد من يستطيع الوصول إليها، وتقليل التعرض غير الضروري للمخاطر. وعليه، فإن الموقف الأكثر اتزاناً للعراق هو اعتماد التدقيق التقني المستقل، ووضع قواعد واضحة لاستخدام التطبيقات في المؤسسات الحساسة، وتطوير قدراته الوطنية في حماية البيانات، مع التمييز الصارم بين الوقائع المثبتة والشكوك التي لم تتحول بعد إلى أدلة.