Millionen von Smartphones in Frankreich verraten mehr, als vielen bewusst ist – besonders für Menschen in sensiblen Berufen. Eine investigative Recherche von *franceinfo* und *L'Œil du 20 heures* zeigt, wie leicht sich aus Geodaten Bewegungsprofile von Militärangehörigen, Geheimdienstmitarbeitern und hochrangigen Politikern rekonstruieren lassen. Eine massive Sicherheitslücke, die alarmierende Fragen aufwirft.

Jeder Schritt nachvollziehbar – ohne Wissen der Betroffenen

„Wie haben Sie meine Daten bekommen? Sie können einfach sehen, wo ich mich bewege?" – Xavier* ist sichtlich irritiert. Die Journalisten, die ihn kontaktieren, wissen bereits, dass er an diesem Donnerstag um 10:57 Uhr in einem Supermarkt in der Drôme war. Um 11:25 Uhr kehrte er nach Hause zurück. Später, um 16:22 Uhr, kaufte er in der örtlichen Bäckerei ein. Am nächsten Morgen verließ sein Handy um 5:46 Uhr das Wohngebiet – auf dem Weg zur Arbeit in das Kernkraftwerk Cruas.

Bevor Xavier überhaupt ans Telefon geht, kennen die Reporter seine Bewegungsmuster genau. Ihre Datenanalyse basiert auf einem Datensatz von 11,7 Millionen Smartphones, deren Standorte über zwei Wochen im Januar 2025 erfasst wurden. Die Ergebnisse sind erschreckend: Nicht nur Privatpersonen, sondern auch Mitarbeiter von Sicherheitsbehörden, Ministerien oder sogar Geheimdiensten hinterlassen unfreiwillig digitale Spuren.

Geodaten: Ein Milliardengeschäft mit gravierenden Folgen

Dass unsere Handys ständig Standortdaten sammeln, ist keine Neuigkeit. Wetter-Apps, Fitness-Tracker, Kleinanzeigen-Portale oder Spiele – viele Anwendungen fordern Zugriff auf den Standort, oft ohne klare Hinweise darauf, wofür diese Daten genutzt werden. Tatsächlich wandern diese Informationen über Werbenetzwerke oder technische Schnittstellen zu sogenannten „Data Brokern" – Unternehmen, die Geodaten in riesigen Mengen aufkaufen und weiterverkaufen.

Ein solcher Datenhändler bot den Journalisten von *L'Œil du 20 heures* kostenlos ein „Testpaket" an: mehr als eine Milliarde GPS-Punkte, erfasst mit metergenauer Präzision und minutengenauer Zeitangabe – quer durch ganz Frankreich. Der Preis für den vollständigen Zugang? Nur ein paar Tausend Euro pro Monat.

„Das Problem ist, dass diese Daten de-anonymisiert werden können“, erklärt Cybersicherheits-Experte Baptiste Robert. „Das erlaubt es, Bewegungsmuster von Menschen in sensiblen Berufen nachzuverfolgen.“ Die potenziellen Risiken sind immens – von gezielter Spionage bis hin zu möglichen Angriffen auf Individuen.

Militärbasen, Geheimdienste, Atomstandorte – nichts bleibt verborgen

Die Untersuchung zeigt, wie leicht sich Einzelpersonen aus anonymen Datensätzen identifizieren lassen. Besonders erschreckend: Die Reporter konnten die Wohnorte von Geheimdienstmitarbeitern, militärischem Personal und Beschäftigten in kritischen Infrastrukturen wie Kernkraftwerken zurückverfolgen.

Auf der Luftwaffenbasis Villacoublay (Yvelines) sind beispielsweise rund 200 Telefone registriert. Ein Nutzer, der hier besonders viele GPS-Punkte hinterlassen hat, lebt in Versailles, geht regelmäßig in einen bestimmten Supermarkt und trainiert in einem nahegelegenen Fitnessstudio. Ganze 7.000 Standortpunkte stammen allein von seinem Gerät.

Noch kritischer: Die französische Marinebasis Île Longue in Brest – Heimat der atomar bewaffneten U-Boot-Flotte. Laut den vorliegenden Daten befanden sich im Januar etwa 50 Handys auf der Insel. Es ist möglich, den täglichen Arbeitsweg eines Offiziers vom Wohnort in Brest über die Fährverbindung bis hin zu den Docks, an denen die U-Boote liegen, nachzuverfolgen. Selbst seine Reisen außerhalb der Bretagne sind sichtbar.

Derartige Analysen setzen sich fort – etwa beim Militärlager Mailly-le-Camp in der Aube. Hier, auf einem Gelände so groß wie Paris, lassen sich über 7.000 GPS-Punkte einzelnen Personen zuordnen. Einer davon ist Philippe*, ein leitender Angestellter der Basis. Sein Standortverlauf zeigt sein Zuhause, seinen Arbeitsweg, aber auch, wann er Besuch von Kollegen hat.

Geheimdienst-Quartier enthüllt – Frankreichs Spione ungeschützt?

Besonders brisant sind die Geodaten aus dem Hauptquartier der *Direction Générale de la Sécurité Extérieure* (DGSE), Frankreichs Auslandsgeheimdienst. Selbst im geheimen Ausbildungszentrum in Cercottes (Loiret) konnten GPS-Punkte einzelnen Personen

---

zugeordnet werden.

Laut *franceinfo* sei es möglich gewesen, Wohnadressen von Mitarbeitern der streng abgeschotteten *Service Action*-Einheit zu rekonstruieren – jener Spezialeinheit, die für geheime Auslandseinsätze verantwortlich ist. Als die Journalisten die DGSE mit ihren Erkenntnissen konfrontieren, gibt es keine offizielle Stellungnahme, lediglich die Bemerkung: „Das ist uns durchaus bekannt."

Ein schwacher Trost – vor allem, wenn man bedenkt, dass ähnliche Datenlecks auch in anderen Ländern existieren. Deutsche Journalisten deckten 2024 auf, dass Mitglieder des Bundesnachrichtendienstes (BND) auf ähnliche Weise identifiziert werden konnten.

Spionagepotenzial: Wer war wann im Élysée-Palast?

Nicht nur das Militär ist betroffen – auch hochrangige Politiker sind ungewollt gläsern. Laut der Analyse befanden sich in einem kurzen Zeitraum mindestens 360 verschiedene Telefone im Élysée-Palast, insgesamt mit 2.600 GPS-Punkten.

Ein Gerät, das regelmäßig dort registriert wurde, lässt sich einem Diplomaten zuordnen. Seine Bewegungen sind klar erkennbar: Von Paris zu einer Präfektur im Süden, von dort weiter in ein Ministerium und später zu einer Botschaft. Auch seine Privatadresse im Val-de-Marne ist leicht aus den Daten herauszulesen.

Das gleiche Muster zeigt sich an anderen Standorten der politischen Macht: Im Innenministerium, im Wirtschaftsministerium oder im Außenministerium wurden insgesamt über 28.000 GPS-Punkte von 2.588 verschiedenen Smartphones aufgezeichnet.

Besonders pikant: Ein Sicherheitsbeamter des französischen Senats konnte identifiziert und bis zu seinem Wohnort in einer östlichen Pariser Vorstadt zurückverfolgt werden. Seine alltäglichen Wege – Supermarkt, Schnellrestaurant – sind detailliert einsehbar.

Was bedeutet das für die Sicherheit?

Diese Enthüllungen sind ein Warnsignal: Nicht nur Bürger, sondern auch Personen mit höchsten Sicherheitsfreigaben sind den Gefahren der Geolokalisierung ausgesetzt. Ein fremder Geheimdienst oder eine kriminelle Organisation könnte dieselben Daten nutzen – für Spionage, Überwachung oder sogar gezielte Angriffe.

In den USA wurde bereits 2024 bekannt, dass Polizeibehörden Zugang zu solchen Daten nutzten, um Bürger zu überwachen, die bestimmte Orte wie Abtreibungskliniken oder religiöse Einrichtungen aufsuchten.

Was also tun? Experten raten dringend dazu, die Standortfreigaben in Apps zu überprüfen und auf ein Minimum zu reduzieren. Auf iPhones lässt sich das unter „Einstellungen > Datenschutz & Sicherheit > Tracking“ deaktivieren. Android-Nutzer finden die Option unter „Einstellungen > Datenschutz > Werbung“.

Denn eines ist sicher: Wer nicht will, dass sein Leben wie ein offenes Buch einsehbar ist, sollte sein Handy nicht zum Geschichtenerzähler machen.

Von C. Hatty