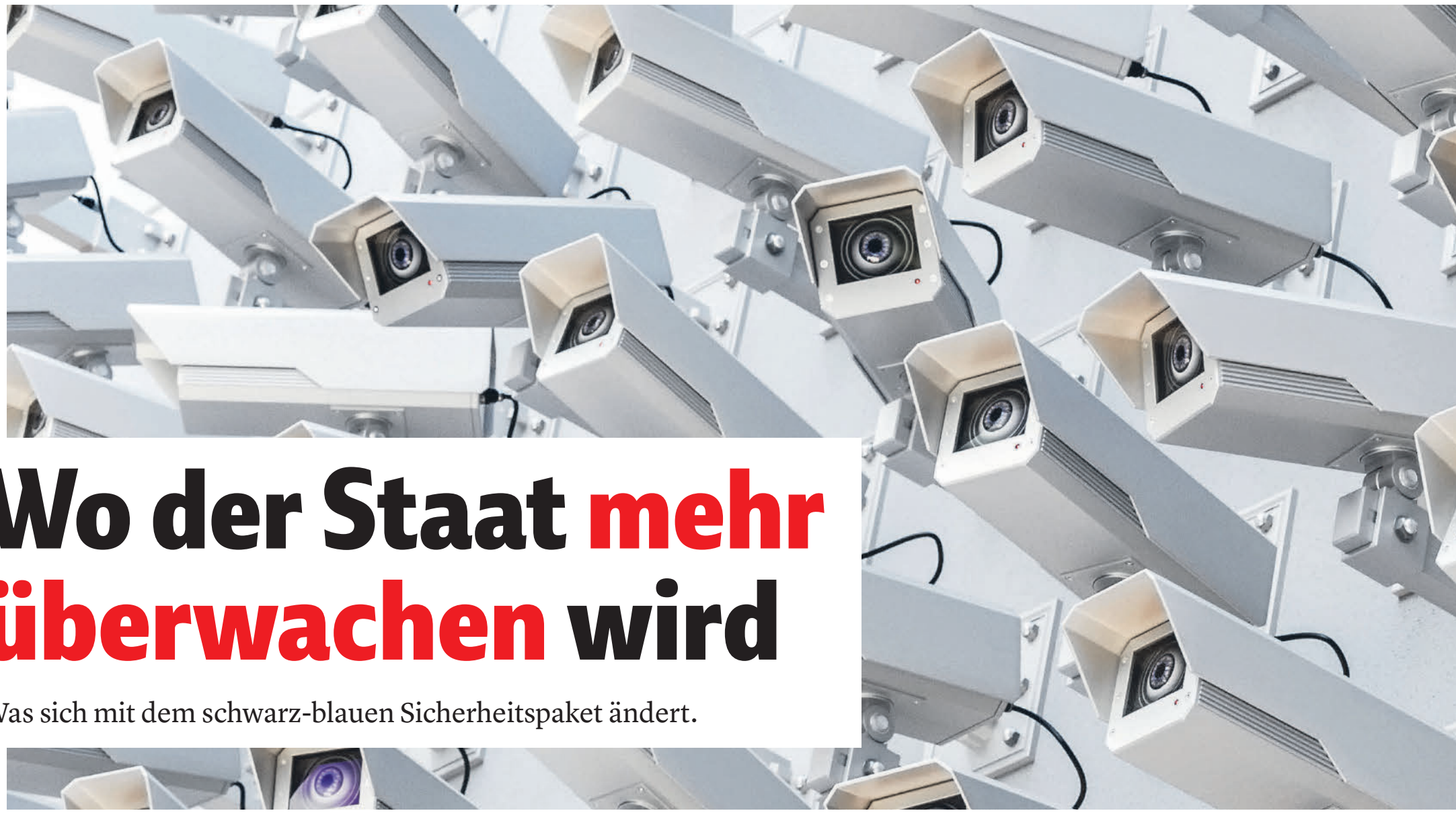

Wo der Staat mehr überwachen wird

Was sich mit dem schwarz-blauen Sicherheitspaket ändert.

WIEN Mehr Überwachung, ein lascheres Briefgeheimnis und eine leichtere Handylokalisierung: Das Sicherheitspaket steht vor seiner letzten Hürde. Der Nationalrat wird den Behörden am Freitag mit schwarz-blauer Mehrheit mehr Befugnisse einräumen. Ein Überblick.

SIM-Karten-Registrierung

AKTUELL Derzeit können Handy-Wertkarten anonym erworben werden, das heißt, die Käufer müssen sich nicht ausweisen.
GEPLANT Ab 2019 müssen sich Kunden auch beim Kauf von Prepaid-SIM-Karten mit ihren Stammdaten registrieren. Für bestehende Kunden ist laut Erläuterungen zum Gesetzesentwurf eine Übergangsfrist geplant. Sie haben bis Mitte Mai 2019 Zeit, ihre persönlichen Informationen nachzuliefern.

Bundestrojaner

AKTUELL Chats in Messenger-Diensten wie WhatsApp können derzeit nicht überwacht werden. Grund dafür ist die „Ende-zu-Ende-Verschlüsselung". Das heißt, nur Sender und Empfänger können die Nachrichten einsehen, der Bote – zum Beispiel WhatsApp – und Dritte nicht. Vergleichbar ist dies mit einem Brief, der in einem Kuvert

„Es kommt es zu einer **Vorratsdatenspeicherung** für den gesamten Straßenverkehr."

Werner Reiter
Epicenter.works

steckt. Bei einer Postkarte hingegen wäre die Nachricht sichtbar.
GEPLANT Messenger-Dienste sollen überwacht werden können. Dafür ist eine Schadsoftware nötig, ein „Bundestrojaner". Voraussetzung ist der Verdacht auf eine terroristische Straftat oder auf eine Tat mit Strafobergrenze von mindestens zehn Jahren bzw. mindestens fünf Jahren, wenn Leib und Leben gefährdet sind. Eine gerichtliche Bewilligung ist notwendig.

Vorratsdatenspeicherung

AKTUELL Bis 30. Juni 2014 mussten Anbieter von öffentlichen Kommunikationsdiensten personenbezogene Daten für sechs Monate speichern, ohne dass diese akut benötigt wurden. Zugriff erhielten die Behörden, wenn die Daten der Aufklärung schwerer Straftaten dienten und eine gerichtliche Bewilligung vorlag. Inhalte der Kommunikation durften nicht gespeichert werden. Die Regel wurde 2014 als verfassungswidrig aufgehoben.
GEPLANT Eine neue Form der Vorratsdatenspeicherung ist geplant. Sie trägt den Namen „Quick Freeze" oder Anlassdatenspeicherung. Sollte ein Anfangsverdacht bestehen, wird eine Speicherung der Telekommunikationsdaten von bis zu einem Jahr möglich. Telekommunikationsanbieter können dazu gezwungen werden. Geografische Einschränkungen oder Begrenzungen auf einen bestimmten Personenkreis gibt es nicht. Für die Datenspeicherung reicht zu Beginn eine Anordnung der Staatsanwaltschaft. Für den Zugriff auf die Daten ist, bei erhärtetem Verdacht, eine gerichtliche Bewilligung nötig.

Kennzeichenerfassung

AKTUELL Die Erkennungsgeräte zur automatischen Kennzeichenerfassung wurden im Jahr 2005 eingeführt. Diese dienen etwa der Prüfung der Vignettenpflicht und der Geschwindigkeitsmessung.
GEPLANT Es sollen zehn stationäre und 20 mobile Kennzeichenerkennungsgeräte angeschafft werden. Auch soll die Polizei Zugriff auf die Autobahnkameras und die Section Control der Asfinag erhalten und nicht nur Autokennzeichen speichern dürfen, sondern auch Informationen, die darüber hinausreichen: von der Automarke über die Farbe hin zu Daten über den Fahrzeuglenker. Eine gerichtliche Bewilligung ist nicht nötig, auch keine vorhergehende Bewilligung durch den Rechtsschutzbeauftragten. Die Daten müssen bis zu zwei Wochen gespeichert werden. Epicenter.works-Datenschützer Werner Reiter spricht von einer Vorratsdatenspeicherung für den gesamten Straßenverkehr und fürchtet eine zu breit angelegte Überwachung.

Briefgemeimnis

AKTUELL Derzeit dürfen Briefe nur beschlagnahmt werden, wenn sich die betroffene Person wegen einer mehr als einjährigen Freiheitsstrafe in Haft befindet oder ihre Festnahme angeordnet wurde. Bei Paketen ist es Zollbeamten jetzt schon möglich, diese auf Verdacht zu öffnen.
GEPLANT Ein Verdacht auf eine vorsätzliche Tat, die mit einer Haftstrafe von über einem Jahr bedroht ist, reicht künftig schon aus, um Pakete und Briefe - nach gerichtlicher Bewilligung und staatsanwaltschaftlicher Anordnung - zu beschlagnahmen.

Ein Auge auf Auto und Bahn

VIDEOÜBERWACHUNG Wer auf Österreichs Autobahnen unterwegs ist, kann sich sicher sein: Spätestens nach ein paar Kilometern fährt er unter einer Videokamera durch. Laut Auskunft der Asfinag sind österreichweit derzeit rund 8300 Kameras im Einsatz, um Autobahnen und Schnellstraßen zu überwachen, und zwar sowohl im Freien als auch in den Tunnels. In Vorarlberg bewachen ungefähr 380 Kameras das hochrangige Straßennetz. Bisher hatte die Polizei keinen Zugriff auf diese Daten. Die Asfinag speichert derzeit nur die Aufnahmen von Rastplätzen und Tunnels, nach 72 Stunden werden die Videos wieder gelöscht. Die Polizei hatte zur Überwachung des Verkehrs und zur Kennzeichenerkennung eigene Geräte im Einsatz. Zukünftig soll die Polizei auch auf gewisse Asfinag-Aufnahmen zugreifen dürfen. Zudem müssen die Videos vier Wochen gespeichert werden. Dazu muss die Asfinag umrüsten. Wie viel, weiß sie noch nicht, wie es auf VN-Anfrage heißt: „Leider gibt's noch keine Details, was die Investitionen betrifft." Kolportiert wird ein niedriger zweistelliger Millionenbetrag.
Auf die Bahn umzusteigen, empfiehlt sich zwar aus Umweltschutz- und Stressgründen, der Überwachung entgeht man aber nicht. An Österreichs Bahnhöfen befinden sich derzeit rund 6000 Kameras, davon 250 in Vorarlberg. Auch in den Zügen befinden sich Kameras. Von 652 Zügen, die in Österreich unterwegs sind, entfallen 21 Nahverkehrsgarnituren auf Vorarlberg. Die Daten werden – je nach Zugtyp – bis zu 96 Stunden gespeichert. Die Videos von den Bahnhöfen sogar für 120 Stunden. ÖBB-Pressesprecher Christoph Gasser-Mair erläutert: „Wenn eine Anzeige vorliegt und die Polizei das Datenmaterial schriftlich anfordert, wird es übergeben." Wie sich das Sicherheitspaket auf die ÖBB auswirkt, sei noch nicht ganz klar. „Denn nicht alle betriebenen Anlagen und Kameras fallen unter die Bestimmungen des Sicherheitspakets", sagt Gasser-Mair. **VN-MIP**

Wie der Staat am Handy mitliest

BUNDESTROJANER Wer mit WhatsApp, Viber, Telegram und Co. kommuniziert, kann davon ausgehen, dass er dies unbeobachtet tut. Die meisten solcher Messengerdienste sind verschlüsselt, im Gegensatz zu Telefongesprächen oder SMS also nicht abhörbar. Die Politik möchte dies ändern, doch das ist technisch gar nicht so einfach. Dazu muss nämlich ein Programm auf dem Handy installiert werden, das heimlich mithört. Dies ist über drei Wege möglich. So wird zum Beispiel zukünftig eine physische Installation möglich sein. Die Verfassungsschützer schnappen sich also das Smartphone und installieren eine geheime Software zum Mitlesen und -hören. Die Alternative dazu ist die Ferninstallation. Wie bei einem Computer funktioniert das über Hackerangriffe, dazu benötigt man einen sogenannten Trojaner. Den Namen erhielt das Programm in Anlehnung an das Trojanische Pferd aus der griechischen Mythologie. In einem Holzpferd versteckt, verschafften sich Soldaten Zugang zur Stadt Troja. So ähnlich funktioniert eine von zwei Möglichkeiten, von außen Zugang zu einem Smartphone zu bekommen. Hacker schicken eine E-Mail mit einer Datei, die als Rechnung oder Dokument getarnt ist. Öffnet man diesen Anhang, installiert sich im Hintergrund der Trojaner. Die Staatsschützer können sich aber auch über Sicherheitslücken im System Zugang zum Smartphone verschaffen. Informationen über diese Lücken müssten sich die Ermittler auf dem Schwarzmarkt besorgen. Gleichzeitig dürften sie die Sicherheitslücke nicht an die Anbieter verraten, sonst wird sie sofort geschlossen. Die Lücken wären also auch für Kriminelle weiterhin offen. Europol und zahlreiche staatliche Geheimdienste fordern schon länger Möglichkeiten, im Bedarfsfall das Smartphone zu überwachen. Kritiker warnen vor dem Trojaner: Dieser könnte die komplette Handynutzung mitlesen, nicht nur die Kommunikation. **VN-MIP**