Legal-Illegal-ganz egal

Stand: 5. Oktober 2024 (EuGH-Urteil Handysicherstellung)
erstellt 11. Dezember 2023

So wird Datenschutz in der EU und damit natürlich auch in Österreich seitens der 'Behörden' verstanden:

Bei den letzten Beschlüssen Ende 2023 wurden seitens EU weitreichende Beschlüsse zur Auflösung des Datenschutzes beschlossen.
Spätestens nach der Europawahl 2024 und rechtzeitig für das Arbeitsprogramm der neuen EU-Kommission Mitte 2024 dürfte es dann mit dem Rest an Datenschutz in der EU endgültig vorbei sein!
Möglich, dass der EuGH noch Teile kippt, aber das ist die Stossrichtung der EU-Kommission und der Wunsch der Mitgliedsländer(!).

> Benjamin Franklin
> Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.
>
> Wer grundlegende Freiheiten aufgibt, um vorübergehend ein wenig Sicherheit zu gewinnen, verdient weder Freiheit noch Sicherheit

Die Bekämpfung von Kriminalität und Terrorismus ist in unseren unsicheren Zeiten leider zu einem umfassenden Kampf mit ungleichen Mitteln geworden!

ABER:

Die Verhinderung privater Kommunikation durch ständige und anlasslose Überwachung schränkt die Meinungsvielfalt und Meinungsfreiheit in einer pluralistischen Gesellschaft ein!
Noch was: eingeschränkter Datenschutz, etwa durch Verbot oder Aufweichung von Verschlüsselung, ermöglicht auch Kriminellen freien Zugang zu Deinen Daten!

Durch die jederzeit mögliche permanente Überwachung, sowohl im öffentlichen Raum, als auch im privaten (Chats) führt dazu, dass Menschen sich Mainstream konform verhalten.
Diese Verhaltensänderung wird als 'chilling effect' bezeichnet.

Ein historischer Rückblick, nur so zum sinnieren:
In Österreich gab es schon mal fast lückenlose Unterdrückung durch Kontrolle unter Staatskanzler Metternich im 19. Jhdt.
Damals gab es starke Einschränkungen hinsichtlich jeglicher politischer Betätigung, kriminelle Recherchen wurden einst mit eher robusten Methoden durchgeführt.
Das Zensurwesen war sehr ausgeprägt. In der *Geheimen Kabinettskanzlei*, dem sogenannten 'schwarzen Kabinett' saßen Beamte, die jeden Brief, jede Mitteilung, jede Zeitung usw. auf versteckte Botschaften penibel lasen.

Die damalige Bespitzelung und Überwachung der Bevölkerung aus Angst vor Umsturz und zum Ausloten der öffentlichen Stimmungslage, führte zu umfassender Zensur und Beschlagnahmen von Post, Zeitungen, Flugblättern, Theater- Opernlibretti usw.

Ein kurzer Blick auf heute: mit dem EU-weit geplanten, permanenten und mit KI gestützen automatischen Mitlesen von Chats, scannen von Cloud und Internet usw. hofft man auch, die 'Stimmungslage' zu erkennen und Abweichler, Ruhestörer oder sonstige gefährliche Terroristen leicht separieren zu können.
Auch die vielfach geforderte 'Altersverifikation' ist ein Baustein, die Anonymität im Netz weiter auszuhebeln. Vorgeschoben werden hier Argumente des Jugendschutzes. In Wirklichkeit steht aber, jeden Nutzer mit seinen aufgerufenen Seiten eindeutig zu markieren. Jugendschutz ist etwas, was Eltern oder sonstige Erziehungsberechtigte den Kindern oder Heranwachsenden verordnen können und altergerecht auch zuteilen sollen!

Zurück in die 'gute alte Zeit', genannt 'Biedermeier':
In Folge führte die allgegenwärtige Einschau des Staatsappaates in die innersten Lebensbereiche zur inneren Emigration der Bevölkerung mit verbundenem Rückschritt.
Letztlich fand diese Unterdrückung ihr Ventil in der Eruption der Revolution von 1848, die blutig niedergeschlagen und bis auf einen Thronwechsel ohne Resultat blieb.

Hier ein Gedicht von Ludwig Pfau (um 1847) dieser 'Biedermeier' Zeit, das die Spießigkeit und Doppelmoral hervorgerufen durch ständige permanente staatliche Kontrolle aufzeigt:

> „Schau, dort spaziert Herr Biedermeier
> und seine Frau, den Sohn am Arm;
> sein Tritt ist sachte wie auf Eier,
> sein Wahlspruch: Weder kalt noch warm.

Damals, 1848, waren die ‚schwarzen Kabinette‘ Metternichs vorbei.
Metternichs Cabinet noir blieb damit aber nur vorerst unbesetzt, keine Regierung kann, schon aus politischen oder militärischen Gründen, auf diese verzichten.

Situation heute:
Ob sich Geschichte wiederholt wissen wir nicht, wenn doch, haben wir zumindest aus damals nichts daraus gelernt.
(von der unseligen NS-Zeit und der brutalen Gleichschaltung aller Medien und Meinungsbildung, Neusprech 'Mainstream', zu berichten, sehe ich hier ab).

Heute sind in der EU die ‚schwarzen Kabinette' fester denn je verankert - man nennt sie nur anders.
Wie schon zitiert, kann keine Regierung, schon aus politischen oder militärischen Gründen, auf diese verzichten.
Neu ist aber, dass sich nun die ganze Bespitzelung anlasslos gegen die gesamte Bevölkerung, also gegen uns alle richtet.

In den ganzen Argumentationen wird immer, ohne es überhaupt in Frage zu stellen, vorausgesetzt, dass es ein behördliches Anrecht darauf gäbe, Bürger überwachen zu dürfen. Wie kommt man darauf und warum sollte es das geben?

Über die wirklichen, und nicht die vorgeschobenen Gründe wie z.B. KiPo, kann man nur spekulieren.
Tatsache bleibt aber, dass es anlasslose allumfassende Überwachnung nur in Diktaturen oder sonstigen faschistischen Systemen gibt.

Sind wir schon wieder so weit?

Verdanken darf man das alles Zensursula und Ylva Johanssen, gesteuert von transatlantischen Influencern ‚Sektierern' wie Ashton Kutcher mit Thorn mit einzigem Interesse für eigene Gewinnmaximierung sowie ‚Sicherheitsbehörden' ohne gesetzlichen Einschränkungen.
Abgenickt wird das ganze dann von Abgeordneten ohne Sachkenntnis.

Wie auch immer, Metternich hätte sich mit seinem 'schwarzen Kabinett', der damaligen Überwachung der Post und seinen Spitzeln über die heutigen Möglichkeiten sicher gefreut!

Chatkontrolle:

In der EU haben sich die Hardliner zur Überwachung von Messenger Diensten (WA, Signal, Threema usw.) unter dem Beifall der Innenminister durchgesetzt.
Treibende Kraft ist die EU-Innenkommissarin Ylva Johansson, die, getriggert auch über US-Organisationen, für ein freies Mitlesen aller Kommunikationsdienste durch die Sicherheitsbehörden eintritt.
Damit kommt auch wieder das Thema 'Vorratsdatenspeicherung' an die Oberfläche.
Alles Wünsche und Träume der Sicherheitsbehörden, denn ohne Verwirklichung dieser ist ja heutzutage wirklich kein Verbrechen mehr aufzuklären! Dieses 'going dark' muss endlich ein für alle mal beendet werden!
Die behaupteten Argumente für behördlichen freien Datenzugriff bleiben immer die gleichen: KiPo, Terrorismus usw. usf.
Glaubt eigentlich irgend jemand ernsthaft, dass in WA der ganze KiPo Dreck verschoben oder gespeichert wird?
Nein, die eigentlichen Gründe der Überwachung sind viel eher, dass diese ein tolles Mittel sind, um die Stimmung in der breiten Bevölkerung automatisiert nach 'Buzz-words' abzuhören. Auch politische Gegner oder Andersdenkende können dann leicht überwacht werden.
Die geforderte Überwachung ist somit alles andere als 'grundlos'.
Neue Kontroll- und Repressionsmöglichkeiten für den staatlichen Sicherheitsapparat sind die offensichtlicheren Gründe.

Wenn dann die Kommunikation einmal kryptografisch 'offen' ist, kann man als nächsten Schritt z.B. verfängliche Bilder oder Texte unliebsamen Personen unterschieben um diese zu diskreditieren und auszuschalten.
Das WIE (z.B. Trojaner oder 'Backdoor') um Verschlüsselung auszuhebeln ist noch nicht entschieden! Das ist ja auch eine 'technische' Sache aus dem Neuland, das Abgeordnete und Minister nicht beantworten müssen und auch nicht können müssen.
Vielleicht wird die Verschlüsselung in Chats künftig auch ganz verboten?
Nur so die Frage eines Laien: glaubt ihr, verehrte Sicherheitsbehörden, wirklich, nachdem die Metadaten ohnehin schon immer 'offen' waren, dass ausser die völlig Blöden Verbrecher WA & Co zum Austausch krimineller Informationen und Botschaften verwenden?
Tipp: Wie wär's mit ein bisschen Steganographie und etwas nachrichtendienstlicher Expertise?
Abhilfe: keinerlei Messenger Dienste verwenden. Derzeit noch für einigermaßen als sicher eingestufte Dienste wie z.B. Telegram oder Signal werden künftig verboten oder datenmäßig unterminiert sein - EuGH Urteil hin oder her.

Gesichtserkennung/biometrische Daten das 'Nummernschild' im Gesicht:

Zur Einstimmung ein Kurzfilm, der das Thema Gesichtserkennung, biometrische Daten und KI wird sehr gut darstellt.
(Der Film 'Reclaim Your Face' ...hol dir dein Gesicht zurück, ist in deutsch)
Kurzfilm von Alexander Lehmann, CC-BY 4.0
https://digitalcourage.video/w/bmBXBcNq1SAKrLRwm11FWH

Was unser EU-Parlament, Rat und Kommission zum Thema mit uns vorhat, lest hier:

(auszugsweise zitiert von Markus Reuter)

> EU-Parlament, Rat und Kommission haben sich 2023 auf die KI-Verordnung unter großem Jubel der Abgeordneten geeinigt. Sie wird trotz angeblicher Schutzmechanismen die automatische Gesichtserkennungn jetzt europaweit etablieren.
> Automatische Gesichtserkennung ist im Prinzip so, als würden wir alle ein gut erkennbares Nummernschild im Gesicht tragen. Ob wir einkaufen, in einen Zug steigen oder auf eine Demonstration gehen – ist die biometrische Technik einmal ausgerollt, sind wir überall über unsere Körperdaten erkennbar und mit Klarnamen unterwegs.
> Dieser düsteren Dystopie einer Zukunft ohne jegliche Anonymität im öffentlichen Raum sind wir mit der Einigung bei der europäischen KI-Verordnung einen gewaltigen Schritt näher gekommen.
> Es droht eine Zukunft, in der niemand mehr im Park sitzen oder sich durch die Stadt bewegen kann – ohne Gefahr zu laufen, dass Gesichtsbiometrie oder andere biometrische Daten permanent gerastert und abgeglichen werden. Das Gefühl, dass wir permanent beobachtet werden, wirkt sich auch auf andere sensible Grundrechte wie die Versammlungsfreiheit aus.

Woher haben die 'Sicherheitsbehörden' unsere biometrischen Daten? In jedem Pass oder Ausweis sind die Fingerabdrücke und die Gesichtsscans abgespeichert. UK verwendet etwa zusätzlich die Fotos von Führerscheinen. Gleichzeitig damit hat auch die Behörde über zentrale Server Zugriff auf diese Daten.

Das US-Unternehmen **Clearview AI** scannt aus dem Internet, fb und anderen 'social media' alle Inhalte nach Gesichtern und zugeordneten Namen. 2023 hat Clearview AI 30 Milliarden Datensätze gespeichert. Ziel des Unternehmens sind 100 Milliarden Datensätze. Weltbevölkerung 2023 sind etwa 8,1 Milliarden Menschen - es sind offenbar viele Gesichter mehrfach in der Datenbank (auch als 'Dateileichen') enthalten.
Es ist als sicher anzunehmen, dass fast alle gespeicherten Daten OHNE Zustimmung der NutzerInnen gesammelt wurden. Abnehmer sind die 'Behörden' in den USA, EU und allen

Staaten die für diese Daten zahlen.
Wo bleibt hier die vielgepriesene DSGVO, wo werden die persönlichen Rechte der Betroffenen gewahrt? Fehlanzeige!
Wie heisst mein Artikel: **Legal - Illegal - Ganz egal**.

Zusätzlich 'sichern' viele 'Handy' Nutzer ihren Zugriff und ihre Daten mittels biometrischer Verfahren (Finger oder Gesichtsscan). Dieser biometrische Abdruck bleibt natürlich NUR am 'Handy' und wird NIEMALS über die Cloud übertragen! Wer's glaubt, möge damit selig werden.

In China ist man bereits einen Schritt weiter: Dort ist die anlasslose Massenüberwachung etabliert und mit 'social scoring' verfeinert worden. Ein Beispiel: Personen, die bei Rot eine Kreuzung überqueren erhalten im social scoring Punkteabzüge. Strafen können automatisiert verhängt werden, Vergünstigungen entzogen werden.
Die chinesische Führung sagt, es sei ein Instrument, um Vertrauen in einer Gesellschaft zu stärken und eine „Mentalität der Ehrlichkeit“ herzustellen.
...so viel Euphemismus für 'anlasslose Rundum Überwachung' muss man erst ertragen können!

Auch die USA sind Vorreiter beim AI-Einsatz durch Sicherheitsbehörden, dort werden Verbrechen schon vorab 'berechnet'.
Dort, im 'land of the free' nennt man das: 'Predictive Policing' für einzelne Personen.
...ich stell' mir das so vor: Du sitzt als couch-potato vor'm TV. Es läutet, die Polizei nimmt dich fest, weil die AI hat berechnet, dass du in einer Stunde einen Terroranschlag verüben wirst!

Ist es DAS, was die EU auch mit uns vor hat?
Abhilfe: Leider keine wirklich praxistaugliche oder legale (Vermummungsverbot).

Weitere, bisher 'denkunmögliche' Methoden zur Überwachung:

Es gibt in D die Überlegungen, in der Cloud eingebundene Sprachassistenten wie Amazon Alexa, Google Home oder Apple Siri ebenso wie 'intelligente' Fernseher, Kühlschränke, Roboter-Staubauger oder Türklingeln, mithin das gesamte IoT (Internet of things) Zeugs anzuzapfen.
'Sicherheitsbehörden' sollen so beispielsweise künftig die Wohnraumüberwachung anlasslos ohne Wissen der Nutzer durchführen können.
Dies sind die Wünsche und Vorstellungen der Behörden in Hessen, Stand Dezember 2023.
Abhilfe: werft allen diesen Schrott aus der idiotischen Datenkrake 'Cloud' - oder wie auch immer diese genannt wird.

Sicherstellung von Datenträgern:

In Österreich wird mit einer Überarbeitung der Beschlagname (gemeint ist die Sicherstellung) von 'Handys' (gemeint sind aber natürlich ALLE Datenträger) seitens Gesetzgeber gearbeitet. Ausgelöst wurde die Debatte seitens VfGH, der Mängel in der Transparenz sah. Das war/ist es aber auch schon.
Auch mit geändertem Gesetz dürfen künftig Datenträger 'Handys' beschlagnamt und ausgewertet werden.
Lediglich ein richterlicher Beschluß und die Information an den Delinquenten wird in dem VfGH Entscheid verlangt.
Sicherstellung nur mit richterlichem Beschluß? Gerne, wird eh alles durchgewunken - es gibt in der österr. Justiz eine 'Bewilligungsstampiglie', also einen Stempel, der alles ligitimiert. Welcher Richter hat schon Zeit für Details!
Diese Beschlagnahme gilt nicht nur für Verdächtige, sondern auch für Personen aus dem Umkreis solcher, oder für Personen, die einfach das Pech haben, im Adressbuch eines Verdächtigen zu stehen.
Verdächtige Zufallsfunde 'Beifang' dürfen natürlich gerne weiter mit ausgewertet werden.
Am nächsten Tag können dann Alle im Boulevard an den intimen Details aus dem Leben einer vielleicht unbescholtenen oder unschuldigen Person teilhaben. Unschuldsvermutung: was ist das?
Auf gut österreichisch: Wir suchen so lang, bis wir irgendwas finden was wir ihm anhängen können. Irgendwas wer ma schon finden, wär doch g'lacht!

Diese Vorgehensweise hat sich die österr. Justiz jetzt vom EuGH absichern lassen!
In dem Urteil C-548/21 des EuGH wird festgestellt: "Die Polizei darf auch dann auf persönliche Handydaten zugreifen, wenn es sich nicht um einen Fall schwerer Kriminalität handelt. Das hat der Europäische Gerichtshof (EuGH) am 4.10.2024 in Luxemburg entschieden.
Siehe: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-10/cp240171de.pdf
...mit diesem Urteil ist es nun also völlig legitim, auch wegen kleiner vermuteter Vergehen, erfunden oder nicht, das abgespeicherte Leben von Delinqenten zu durchforsten. Nicht auszudenken, wenn damit auch Meinungen zu politischen Themen kriminalisiert werden.
Soweit zu: "Ich habe nichts zu verbergen!"

Abhilfe: kein Smartphone 'Handy' verwenden. Wo keine Daten vorhanden sind, kann auch nichts gefunden werden.
Sonstige 'Datenträger': Wichtige oder 'heikle' Inhalte verschlüsseln mittels PGP, VeraCrypt oder 7zip mit AES-256. Noch gibt es quelloffene Verschlüsselungsprogramme. Die Folter zur Herausgabe von PW ist halt auch in der EU (noch) nicht möglich!
Alternative Möglichkeiten mit und ohne Internet verwenden.

Quellen (Links) und Pressespiegel 2024 (neueste zuerst)

Sicherstellung von Datenträgern, Mobiltelefonen 'Handy'
In einem Urteil des EuGH wird auf Anfrage der österr. Justiv festgestellt: "Die Polizei darf auch dann auf persönliche Handydaten zugreifen, wenn es sich nicht um einen Fall schwerer Kriminalität handelt. Das hat der Europäische Gerichtshof (EuGH) am 4.10.2024 in Luxemburg entschieden.
https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-10/cp240171de.pdf

Artikel (nur eine kleine Auswahl):

https://www.krone.at/3548711
https://www.diepresse.com/18930998/eugh-polizei-darf-auf-persoenliche-handydaten-zugreifen?ref=ues_a
https://www.golem.de/news/eugh-urteil-polizeilicher-zugriff-auf-handydaten-unter-auflagen-erlaubt-2410-189531.html

Damit ist das Urteil des österr. Verfassungsgerichtshofs ausgehebelt.
https://www.vfgh.gv.at/medien/Sicherstellung_Datentraeger.php
Ab diesem EuGH Urteil vom 4.Okober 2024 gilt: Legal-Illegal-ist uns scheissegal

...mit diesem Urteil ist es nun also völlig legitim, auch wegen kleiner vermuteter Vergehen, erfunden oder nicht, das abgespeicherte Leben von Delinqenten zu durchforsten. Nicht auszuschliessen, dass damit auch ungewünschte Meinungen zu politischen Themen kriminalisiert werden.
Soweit zu: "Ich habe nichts zu verbergen!"

Nach diesem EuGH Urteil: Unternehmt ALLES zu eurem persönlichen Datenschutz, schützt eure 'Privatsphäre', denn die Justiz (die Behörde) darf nach diesem EuGH Urteil jeden von euch jederzeit durchleuchten und ALLES auswerten!
Richterliche oder gleichwertige Kontrolle ist nach EuGH notwendig - Muahahah, wir, die Behörde sind das Gesetz.

Wenn es euch NICHT egal ist, und ihr eure Privatheit schützen wollt, dann setzt Gegenmassnahmen wie:
Datenvermeidung (z.B. keine social media, keine Messenger Dienste wie WA usw.) Daten und Datenträger mit PGP, VeraCrypt oder 7zip mit AES-256 verschlüsseln, soweit dies irgend möglich ist und natürlich keine 'Klaut' (Cloud).
Auf gut österreichisch: Wo nix is, is nix!

Biometrische Gesichtserkennung abwehren
Wer Kameras entgehen will, hat es zunehmend schwer. Dabei genügt ein Schnappschuss, um einen Menschen zu identifizieren. Wir erkunden die faszinierende Welt des Widerstands gegen biometrische Erkennung.

> Anmerkung: Zusammengefasst, wir habe keine Chance diesem Überwachungsirrsinn zu entgehen.
> Offenbar gibt es keinerlei Tabus, Grenzen oder „rote Linien“ mehr.
> Was technisch irgendwie gemacht werden kann wird gemacht.
> Grundrechte, Rechtmäßigkeit, Demokratie, Rechtsstaat, usw… interessiert das die Politiker oder irgendjemand sonst überhaupt noch?

https://netzpolitik.org/2024/digitale-selbstverteidigung-biometrische-gesichtserkennung-abwehren/

Messenger Überwachung in Österreich
Aus Anlass eines gerade noch rechtzeitig verhinderten geplanten Terroranschlags durch islamistische Terroristen sollen Messenger durch die Behörden mitgelesen werden können.

Strafrechtsprofessorin Ingeborg Zerbes hält eine gezielte Chat-Überwachung für grundsätzlich verfassungskonform.
Zerbes, die Vorsitzende der Kontrollkommission des Staatsschutzes ist, kenne "den Rahmen des Entwurfs" und hält den Einsatz der Messenger-Überwachung bei schwerwiegenden Delikten wie geplanten Terroranschlägen für "sinnvoll".

> Anmerkung: Als 'schwerwiegend gelten nach Zerbes z.B. Terror und verfassungsgefährdende Verbrechen. Diese Definition mag im Schlaglicht eines verhinderten Anschlags als zwingender Handlungsbedarf (Anlaßgesetzgebung) gesehen werden. Es gibt aber in Österreich die Tradition, ALLES gefundene auszuwerten und dem Boulevard zuzuspielen, auch dann, wenn die Verdachtsperson unschuldig ist.
> Wie wäre eine rigorose Abschiebung solcher Terroristen aus Österreich UND eine Aufnahme von islamistischen Gewaltphantasien in das 'Verbotsgesetz', in dem z.B. auch NAZI Propaganda strikt bestraft wird. Damit könnte auch eine Löschung in den (asocial) Medien wie TikTok durchgesetzt werden!

Behörden sollen Chats mitlesen dürfen – das steht im Entwurf für die Messenger-Überwachung
Bei "verfassungsgefährdenden Angriffen" soll auf Handys von Verdächtigen Überwachungssoftware eingeschleust werden. Die rechtlichen Grenzen sind eng
Der Standard Jakob Pflügl 13. August 2024
https://www.derstandard.at/story/3000000232232/chat-ueberwachung-geht-in-begutachtung-das-sind-die-rechtlichen-knackpunkte

Was das deutsche Innenministerium zur Gesichtserkennung plant

Künftig sollen Polizeibehörden Bilder von Verdächtigen mit dem Internet abgleichen können, um sie zu finden. Dieser Vorschlag aus dem Innenministerium ist ein Albtraum für Grundrechte.
13.08.2024 um 15:14 Uhr - Tomas Rudl, Anna Biselli
Anmerkung: Datenabgleich z.B.: mit Clearview AI !!!
https://netzpolitik.org/2024/nancy-faeser-was-das-innenministerium-zur-gesichtserkennung-plant/

Chatkontrolle: Abstimmung ausgesetzt

Die Abstimmung über die Chatkontrolle der belgische Ratspräsidentschaft ist gescheitert. Es konnte keine Mehrheit der EU-Staaten 'sondiert' werden.
Deshalb hat die belgische Ratspräsidentschaft darüber auch keine offizielle Abstimmung durchgeführt, um einer Ablehnung zu entgehen.
Leider ist das Gesetz dadurch noch lange nicht vom Tisch, der Kampf geht weiter.
Spätestens mit Übernahme der Ratspräsidentschaft durch Ungarn wird das Ringen um die Chatkontrolle weitergehen.

Eine Zusammenfassung von Artikeln zur Chatkontrolle von **Netzpolitik.org** findest Du hier:
Heute feiern, morgen weiter kämpfen
20.06.2024 um 17:41 Uhr - Andre Meister, Maximilian Henning

https://netzpolitik.org/2024/reaktionen-zur-chatkontrolle-heute-feiern-morgen-weiter-kaempfen/

der Kontroll- und Abhörwahnsinn geht auch 2024 weiter...
Für mich eine gruselige Vorstellung - wohin ist bloß unsere Freiheit angstfrei und ohne Überwachung zu kommunizieren, entschwunden?

EU-Expertengruppe fordert Hintertüren und mehr Überwachung
https://netzpolitik.org/2024/going-dark-eu-expertengruppe-fordert-hintertueren-und-mehr-ueberwachung/
Markus Reuter 05.06.2024
Kann die Polizei in Zeiten von Verschlüsselung noch gut ermitteln? Eine Expertengruppe der EU sollte dazu Empfehlungen abgeben und fordert jetzt Hintertüren zu verschlüsselten Nachrichten und viele weitere Überwachungsmöglichkeiten. Wir veröffentlichen die eingestuften Empfehlungen des von Sicherheitsbehörden dominierten Gremiums.

Zitate:
Was ist eigentlich, wenn Nordkoreanische oder Russische Staatshacker diese „Hintertüren“ dann finden, ausnutzen und unsere gesamte digitale Infrasruktur damit lahmlegen ?

Verschlüsselung: Polizei will in Echtzeit an Datenströme von WhatsApp & Co.
https://www.heise.de/news/Verschluesselung-Polizei-will-in-Echtzeit-an-Datenstroeme-von-WhatsApp-Co-9747785.html
Stefan Krempl 04.06.2024
Zitate:
Das ist ein Instrument für Diktaturen um die Menschen zu kontrollieren und davon abzuhalten aufzubegehren, so etwas brauchen wir in Demokratien nicht!

Zusammengefasst würde das zu einer permanenten und lückenlosen Überwachung der gesamten Gesellschaft in allen Bereichen des Lebens mit all ihren technischen und sozialen Gefahren führen. Jeder mit Gesundem Menschenverstand kann sich ausmalen was alles unter diese Gefahren fällt.

Never ending story: Chatkontrolle & EU-Bürgerrechte
17.04.2024 um 13:12 Uhr - Markus Reuter, Andre Meister
…Verschlüsselte Dienste sollen als erstes durchleuchtet werden.
Aus Dokumenten der belgischen EU Ratspräsidentschaft geht hervor, dass sichere und die Privatsphäre schützende Dienste besonders im Visier der geplanten Chatkontrolle stehen sollen(!)
Nach dem Motto „Je sicherer, desto mehr Chatkontrolle“ führen Sicherheitsfeatures wie Anonymität oder Ende-zu-Ende-Verschlüsselung dazu, dass eine andere (höhere) Risikobewertung vorgenommen wird.

…datenschutzfreundlich anonym nutzbare Kommunikationsdienste wie Protonmail sollen per Verpflichtung zur Chatkontrolle zu den extremüberwachtesten Diensten werden.
Ausgerechnet die bisher sicher verschlüsselten Messengerdienste wie Signal sollen durch verpflichtendes ‚client-side scanning‘ zu Spionen auf unseren Smartphones werden.
https://netzpolitik.org/2024/chatkontrolle-verschluesselte-dienste-sollen-als-erstes-durchleuchtet-werden/

NB: Bin schon gespannt, wie das ausgehen wird. Ob der EU-Gerichtshof die Vorschläge der EU-Kommission zur anlasslosen und massenhaften Chatkontrolle absegnen wird?

Aushebelung der Verschlüsselung für alle Messenger Dienste
16.04.2024 ORF ZIB2
Haijawi-Pirchner DSN:
...Das internationale Vertrauen in seine Behörde sieht Haijawi-Pirchner durch die Spionageaffäre nicht gefährdet. Auf Informationen von internationalen Partnern sei man teilweise auch angewiesen, gebe es in Österreich doch keine Möglichkeit der Überwachung von Messenger-Diensten, warb er erneut für eine Ausweitung der Kompetenzen.
Die Abfrage der Verbindungsdaten wie von Alma Zadić Justizministerin (Grüne) vorgeschlagen, reiche nicht.

Eine solche (gesamte) Überwachung hatte auch Innenminister Gerhard Karner (ÖVP) immer wieder gefordert. Vor Kurzem hieß es allerdings, dass diese lediglich Metadaten betreffen solle - für Haijawi-Pirchner ist das allerdings nicht ausreichend. Bei einzelnen Gefährdern und Gefährderinnen müsse man auch die verschlüsselte Kommunikation überwachen (also in Klartext mitlesen) können.

Mein OptOut: Da kein 'bisschen Verschlüsselung' möglich ist, und offenbar Hintertüren zur Umgehung gefordert werden, Messengerdienste komplett meiden oder nur für untergeordnete Kommunikation wie: "bei dir auch schönes Wetter?" verwenden.

Privatsphäre für alle oder niemanden
23.03.2024
Die Taurus-Abhöraffäre zeigt eines sehr deutlich: Verschlüsselte und sichere Kommunikation funktioniert nicht für einige wenige. Stattdessen muss sie zum Standard für alle werden.
Ein Kommentar von Gastbeitrag, Meredith Whittaker (Signal-Chefin)
https://netzpolitik.org/2024/taurus-abhoeraffaere-privatsphaere-fuer-alle-oder-niemanden/
...der Hinweis im Titel auf die Taurus-Affäre ist mM eher eine irreführende Intro!
Ein HERVORRAGENDER Artikel zum Thema Datenschutz!

Going Dark: Zivilgesellschaft gibt Kontra
21.02.2024
Eine Expert:innengruppe der EU debattiert derzeit, wie Ermittlungsbehörden an mehr Daten gelangen können.
https://netzpolitik.org/2024/going-dark-zivilgesellschaft-gibt-kontra/

KI-Verordnung erhält grünes Licht

02.02.2024

Die EU-Mitgliedstaaten haben heute den Kompromisstext der KI-Verordnung bestätigt. Das größte Regelwerk der Welt für Künstliche Intelligenz wird damit wahrscheinlich noch vor den EU-Wahlen in Kraft treten – ungeachtet der breiten Kritik am gesetzgeberischen Prozess und an der drohenden Massenüberwachung.

Ergänzungen lesen!

...Anonym schreiben, weil in einer EU die Veröffentlichung der eigenen Meinung bereits gefährlich geworden ist.

https://netzpolitik.org/2024/eu-rat-ki-verordnung-erhaelt-gruenes-licht/

Die sieben quälendsten Fragen zur KI-Verordnung

26.01.2024

Wieso hagelt es jetzt so viel Kritik? Wie schlimm wird das mit der Gesichtserkennung? Und was lässt sich jetzt überhaupt noch machen? Wir liefern die wichtigsten Updates zur fast fertigen KI-Verordnung.

1. Die Einigung war doch vor Weihnachten, wieso hagelt es jetzt Kritik?
2. Gesichtserkennung: Wie schlimm wird es?
3. Emotionserkennung: Was droht hier?
4. Migrationskontrolle: Wie schlimm ist es?
5. Nationale Sicherheit: Was dürfen Staaten alles machen?
6. Ist an dem Gesetz auch irgendetwas gut?
7. Lässt sich jetzt überhaupt noch etwas ändern?

https://netzpolitik.org/2024/grundrechte-in-gefahr-die-sieben-quaelendsten-fragen-zur-ki-verordnung/

Sekte macht Lobbyarbeit pro Chatkontrolle
02.02.2024 Christoph Schmees
(zum Thema EU-Lobbying mit Ashton Kutchers Thorn)
...Zu den vehementen Verfechtern der Chatkontrolle gehört die angeblich gemeinnützige Organisation Thorn eines gewissen Ashton Kutcher. Dahinter steckt eine gefährliche Sekte, die sich selbst als Kirche bezeichnet, aber einen eigenen Geheimdienst besitzt. Wer bisher vielleicht noch dachte, dass an der Chatkontrolle irgendetwas gutes wäre, weiß spätestens jetzt: Ein Vorhaben, das solche Fürsprecher hat, kann niemals gut sein.
https://www.pc-fluesterer.info/wordpress/2024/02/02/sekte-macht-lobbyarbeit-pro-chatkontrolle/

Thorn brachte Chatkontrolle auch für andere Themen ins Spiel
26.01.2024
...ein beängstigender Artikel darüber, was die Zukunft bringen wird!
Ashton Kutchers Organisation Thorn war von Anfang an der Entstehung der Chatkontrolle-Verordnung beteiligt. Neue Dokumente zeigen, mit welchen Aussagen Thorn die EU-Kommission lobbyiert hat – unter anderem verwies die Organisation auch auf die Möglichkeiten der Chatkontrolle abseits des Kampfes gegen Kindesmissbrauchs.
https://netzpolitik.org/2024/verschluesselung-thorn-brachte-chatkontrolle-auch-fuer-andere-themen-ins-spiel/

Sicherheitsrisiko: So einfach können Handy-Nutzer heimlich verfolgt werden
12.01.2024
https://www.heise.de/news/Sicherheitsrisiko-So-einfach-koennen-Handy-Nutzer-heimlich-verfolgt-werden-9596230.html

Biometrische Massenüberwachung ohne Wenn und Aber?
12.01.2024
Nachträgliche Änderungen bei der biometrischen Überwachung sorgen aktuell für Ärger bei EU-Abgeordneten, die bis zuletzt für eine Einschränkung gekämpft hatten. Wird das Gesetz in der nun vorliegenden Form verabschiedet, hätte dies dramatische Folgen.
https://netzpolitik.org/2024/ki-verordnung-biometrische-massenueberwachung-ohne-wenn-und-aber/

Panoptischer Rewe-Supermarkt

Einkauf mit Skelettkontrolle

13.01.2024

...Grundsätzlich werden in solchen Supermärkten alle Kund:innen von den Überwachungssystemen erfasst, verfolgt und gespeichert – auch wenn sie ganz herkömmlich einkaufen und am Kassenband bezahlen.

...Die erhobenen Aufnahmen werden laut Rewe verpixelt bei einem Cloudanbieter auch außerhalb der EU gespeichert und mittels „künstlicher Intelligenz“ ausgewertet.

https://netzpolitik.org/2024/panoptischer-rewe-supermarkt-einkauf-mit-skelettkontrolle/

Quellen (Links) und Pressespiegel 2023

anlasslose Massenüberwachung:
EU berät über "Going Dark": Hinter verschlossenen Türen
(7 Ergänzungen)
Thomas Rudi 11. Dez. 2023
https://netzpolitik.org/2023/eu-beraet-ueber-going-dark-hinter-verschlossenen-tueren/

Beim Verbot der Massenüberwachung darf es keine Ausnahmen geben
Peter Zellinger 10. Dez. 2023
Europa feiert sich für den AI Act. Dabei erlaubt die Union den nationalen Behörden, verbotene Technologie gegen ihre Bürgerinnen und Bürger einzusetzen
https://www.derstandard.at/story/3000000198930/beim-verbot-der-massenueberwachung-darf-es-keine-ausnahmen-geben

Biometrische Gesichtserkennung:
KI-Verordnung: Das Nummernschild im Gesicht kommt
Markus Reuter 11. Dez. 2023
Ein Kommentar
https://netzpolitik.org/2023/ki-verordnung-das-nummernschild-im-gesicht-kommt/

'Your Face Belongs to Us - story about Clearview AI'
New York Times journalist Kashmir Hill
https://www.theverge.com/23919134/kashmir-hill-your-face-belongs-to-us-clearview-ai-facial-recognition-privacy-decoder

Gesichtserkennung: 50 Millionen Führerscheinbilder für die britische Polizei
24.12.2023
Mit einer von der britischen Regierung heimlich eingeführten Gesetzesnovelle dürften Ermittler per Gesichtserkennung die Führerschein-Datenbank durchsuchen.
https://www.heise.de/news/Gesichtserkennung-50-Millionen-Fuehrerscheinbilder-fuer-die-britische-Polizei-9582385.html

Social Scoring:
Diese Systeme kriechen in unseren Alltag.
13.03.2023
https://www.tagesspiegel.de/gesellschaft/diese-systeme-kriechen-in-unseren-alltag-4046119.html

Handy Sicherstellung und Durchsuchung:
Österreich: Handydurchsuchung ohne Gerichtsbeschluss ist verfassungswidrig
20.12.2023
https://www.heise.de/news/Oesterreich-Handydurchsuchung-ohne-Gerichtsbeschluss-ist-verfassungswidrig-9579052.html

„Mit der Zeit gehen“ Sicherstellung von Datenträgern
23.12.2023
Die ÖVP macht bei Handy-Sicherstellung Druck
https://www.krone.at/3201935

Deutschland denkt schon weiter...
Polizeibefugnis: CDU und SPD in Hessen wollen digitale Wanzen im Wohnzimmer
https://www.heise.de/news/Polizeibefugnis-CDU-und-SPD-in-Hessen-wollen-digitale-Wanzen-im-Wohnzimmer-9577621.html

Clearview AI and the end of privacy, with author Kashmir Hill
NY Times Journalist
17. Oktober 2023
Your Face Belongs to Us, and what the spread of facial recognition technology means for the future of privacy
https://www.theverge.com/23919134/kashmir-hill-your-face-belongs-to-us-clearview-ai-facial-recognition-privacy-decoder