KULTUR NEU ENTDECKEN

SWR2

SWR2 Wissen

Überwachungstechnik für Diktatoren

Wie die EU den Export bremsen will

Von Thomas Kruchem

Sendung: Dienstag, 6. April 2021, 8.30 Uhr
Redaktion: Gábor Páal
Regie: Thomas Kruchem
Produktion: SWR 2021

Mit Spähsoftware und intelligenter Videoüberwachung kann man Terroranschläge verhindern – aber auch Regimegegner kontrollieren. Der Export dieser Techniken ist kaum geregelt.

MANUSKRIPT

Autor:
Das niederländische Unternehmen *Noldus* hat eine Software namens *FaceReader* entwickelt. Sie erkennt in einem Gesicht Gefühle: Glück zum Beispiel, Angst, Ärger, Ekel, Überraschung. Mit *FaceReader* kann man erkennen, ob ein Alzheimer-Patient unter Schmerzen leidet oder ob ein Pilot einen Schwächeanfall hat. Dieselbe Software erkennt aber auch, ob ein Regimegegner in einem Verhör lügt. Darf also eine solche Technik in autoritär regierte Staaten geliefert werden?

Ansage:
Überwachungstechnik für Diktatoren. Wie die EU den Export bremsen will. Von Thomas Kruchem.

Autor:
Die Firma *Noldus* hat ihr Programm zur Emotionserkennung auch nach China geliefert, an die Universität von Xinjiang etwa – in eine Region, wo Hunderttausende muslimische Uiguren in Umerziehungslagern interniert sind. Ein absolutes *no go* aus der Sicht von Lena Rohrbach, Expertin für Überwachungstechnik bei *Amnesty International*.

O-Ton Lena Rohrbach:
In China wird staatliche Videoüberwachung auch mit Gesichtserkennung in rasendem Tempo ausgebaut. Und da handelt es sich einmal um die großangelegten chinaweiten Massenüberwachungsprogramme – zum Beispiel *Skynet* oder *Sharp Eyes*, die dann durch Videoaufzeichnung und zunehmend auch automatisierte Analyse das öffentliche Leben aufzeichnen.

Musikakzent

Autor:
Produkte wie die Noldus-Software *FaceReader* sind keine Rüstungsgüter, für die es aus guten Gründen Exportbeschränkungen gibt. Es handelt sich vielmehr um Produkte, die zwar in Militär und Polizei zum Einsatz kommen können, sich aber genauso gut für zivile Zwecke nutzen lassen. Sie heißen deshalb *Dual use*-Produkte.

Viele Güter fallen in diese Kategorie. Etwa Ammoniumnitrat, aus dem man Dünger herstellen kann – oder Sprengstoff; Lastwagen, mit denen man Getreide transportieren kann – oder Munition; und eben: Überwachungstechnik, mit der man Terroranschläge verhindern oder Oppositionelle kontrollieren kann. Den internationalen Handel mit solchen Produkten regelt das sogenannte *Wassenaar*-Abkommen von 1995. Dessen Listen exportbeschränkter Güter hat die EU eins zu eins übernommen.

Das Problem: Überwachungstechnologie findet sich kaum auf diesen Listen. Ihr Export ist somit kaum geregelt. EU-Firmen exportieren deshalb bis heute fast unbegrenzt Überwachungstechnik in autoritär regierte Länder; und EU-Institutionen schulen deren Sicherheitskräfte beim Umgang mit der Technik.

Immerhin: Seit 2016 reformiert die EU ihre sogenannte *dual-use*-Verordnung. Sie soll künftig auch Überwachungstechnik umfassen, sofern mit ihr Menschenrechte verletzt werden können.

So wie im Fall des marokkanischen Menschenrechtsaktivisten Maati Monjib. Er lehrt und forscht als Historiker an der Universität „Mohammed V." in Marokkos Hauptstadt Rabat.

O-Ton Maati Monjib, darüber Übersetzung:
An einem Vormittag im März 2020 fuhr ich mit einem Studenten in meinem Auto nach Rabat. Wir sprachen über den Fortgang seines Studiums; und er fragte mich, wie er eine Doktorandenstelle in den USA ergattern könne. „Du musst dort- und dorthin schreiben und dich bewerben", sagte ich dem Studenten. Zwei Tage später berichtete dann *Chouf TV*, ich hätte Geld von dem Studenten bekommen, um seine illegale Auswanderung in die USA zu organisieren.

Autor:
Er werde seit Jahren engmaschig überwacht, sagt Maati Monjib – im Auto, in seiner Wohnung. Und der staatsnahe Online-Sender *Chouf TV* verbreite bösartig Zusammengeschnittenes aus Monjibs Privatgesprächen.

Musikakzent

Autor:
Mit Überwachungstechnik aller Art drangsaliere Marokkos Regierung Menschenrechtler, Oppositionelle und Journalisten, berichten Menschenrechtsorganisationen wie *Amnesty International* und *Reporter ohne Grenzen*. In anderen autoritär regierten Ländern geschehe Ähnliches.

Zur Technik für verdeckte Überwachung zählen sogenannte *Trojaner*, die, getarnt als harmlose Apps, auf Smartphones und Notebooks gelangen. *Trojaner* können Mikrofon, Kamera und GPS aktivieren, ohne dass der Nutzer es merkt. Sie können sein Bewegungsprofil erstellen und seinen gesamten Telefon- wie Datenverkehr absaugen. Andere Spähsoftware dient der Massenüberwachung: Sie identifiziert im Internet Oppositionelle und deren Posts. Sogenannte *IMSI-Catcher* sind Geräte, die sämtliche Smartphone-Nutzer in ihrer Nähe erfassen – und deren Daten- wie Telefonverkehr.

Und die Liste der Überwachungstechniken lässt sich fortführen: Programme, die bestimmte Internetseiten sperren, gehören dazu; hochauflösende Kameras, die den öffentlichen Raum überwachen – und Gesichtserkennungstechnologie, die aus Millionen Menschen diejenigen herausfiltert, die interessant sein könnten für die Behörden. Überwachungstechnik sei heute ein *must buy* für Diktatoren weltweit, meint Stéphane Chardon, leitender Exportkontrolleur der EU-Kommission. EDV-gestützte Überwachungstechnik sei einfach effizienter, eleganter und billiger als Tränengas, Wasserwerfer oder Spitzel.

O-Ton Stéphane Chardon, darüber Übersetzung:
Der Handel mit diesen Produkten boomt – in praktisch allen Ländern der Erde. Und involviert sind neben Regierungen dubiose private Akteure, Kriminelle und

Terroristen. Die Preise für Überwachungstechnik wird immer billiger und damit immer leichter erhältlich. Technik, die vor zehn Jahren nur wenigen Geheimdiensten zugänglich war, nutzen heute zahllose Akteure weltweit.

Autor:
Während die Preise sinken, steigen die Umsätze. Insbesondere Gesichtserkennungstechnologie ist gefragt. Nach einer Schätzung des Online-Portals „Markets and Markets“ dürfte der Umsatz damit von 3,8 Milliarden US-Dollar 2020 auf 8,5 Milliarden Dollar 2025 steigen.

Die meisten Produzenten dieser und anderer Überwachungstechnik sitzen in den USA, Israel und der EU. Das wohl bekannteste deutsche Produkt ist der *Trojaner Finspy* des Münchener Unternehmens *FinFisher*. *Finspy* wurde in fast allen arabischen Ländern und der Türkei gefunden. Weil es an den nötigen Ausfuhrgenehmigungen fehlt, ermittelt seit 2019 die Staatsanwaltschaft.

Atmo:
Trovicor-Video

Autor:
Das gleichfalls in München ansässige Unternehmen *Trovicor* zeigt im Internet dramatische Szenen, in denen seine Abhör-Software *Monitoring Center* Terroristen zur Strecke bringt – gerade noch rechtzeitig, bevor Schlimmeres geschieht. Für Menschenrechtsaktivisten allerdings ist *Trovicor* mit seinen Filialen in Dubai, Islamabad und Kuala Lumpur ein rotes Tuch. Die Abhörsoftware des Unternehmens wird immer wieder in Ländern gefunden, wo die Regierungen regelmäßig Menschenrechte verletzen. Welche und wie viele Menschen dort mit *Monitoring Center* abgehört werden, lässt sich technisch schwer feststellen, weil die Software Kommunikationsdaten nicht von einzelnen Geräten, sondern aus Datennetzen abgreift. Ein grundsätzliches Problem bei vielen Produkten der Überwachungstechnologie. Immer mal wieder jedoch wird eine Spähsoftware auch identifiziert.

Atmo:
Bericht *Semana*

Autor:
In Kolumbien zum Beispiel: Im Mai 2020 veröffentlichte die auch online publizierte Wochenzeitschrift *Semana* Dokumente über ein Spähprojekt des militärischen Geheimdienstes. Dabei sei auch die Software einer europäischen Firma eingesetzt worden, erklärt Lisa Dittmer, Sprecherin der Organisation *Reporter ohne Grenzen*.

O-Ton Lisa Dittmer:
Die heißt *Mollitiam Industries*; und die hat wohl in den letzten Jahren Spähsoftware-Systeme an das kolumbianische Militär geliefert, mit dem dieses Militär dann unter anderem prominente Richterinnen und Richter und auch Journalisten abgehört hat.

Autor:
Im Herbst 2020 schließlich berichtet *Amnesty* über drei EU-Unternehmen, die den chinesischen Sicherheitsbehörden geholfen haben, ihre Massenüberwachung

auszubauen: Das schwedische Unternehmen *Axis Communications* habe hochauflösende Netzwerk-Kameras für die Videoüberwachung geliefert, die französische Firma *Idemia* modernste Gesichtserkennungstechnologie. Und das eingangs erwähnte niederländische Unternehmen *Noldus* Software zur Emotionsanalyse.

Insbesondere *Noldus* wehrt sich allerdings vehement gegen die Behauptung, es stärke mit seinem Produkt den Überwachungsstaat in China. In einer Stellungnahme gegenüber SWR2 Wissen schreibt *Noldus*-Chef Lukas Noldus.

Zitat Lucas Noldus:
In den mehr als 30 Jahren, die wir Forschungssoftware entwickeln, haben wir nicht einmal erlebt, dass mit unserer Software Menschenrechte verletzt wurden. Dennoch verlangen wir beim Verkauf an Militär- und Polizeibehörden stets eine unterschriebene Erklärung über die Endnutzung unserer Produkte, der ich als *Noldus*-Chef zustimmen muss.

Autor:
Lucas Noldus verweist auf die Anwendungsmöglichkeiten der Emotionserkennung in der Medizin. Bitter fügt er hinzu:

Zitat Lucas Noldus:
Amnesty sagt im Grunde, europäische Firmen sollten China nicht helfen, das Leid von Alzheimer-Patienten zu lindern und die Sicherheit in der Luftfahrt zu verbessern.

Musikakzent

Autor:
Das Beispiel der *Noldus*-Software zur Emotionsanalyse zeigt die Janusköpfigkeit vieler Überwachungsprodukte: Einerseits können sie medizinischen Zwecken oder legitimen Sicherheitsinteressen dienen; andererseits können Sie Menschenrechte verletzen und Diktaturen stabilisieren. Die Entscheidung, ob ein solches Produkt exportiert werden darf, ist deshalb im Einzelfall kompliziert; bei der Abwägung sind viele Aspekte zu beachten. Dass die Gefahr des Missbrauchs der Technik nicht zu unterschätzen ist, zeigen Erlebnisse von Überwachungsopfern – wie dem Historiker und Menschenrechtsaktivisten Maati Monjib in Marokko.

Atmo:
Cjouf TV

Autor:
Bösartige Karikaturen von Maati Monjib präsentiert der marokkanische Online-Sender *Chouf TV* auf *YouTube* – Monjibs Krallen voller Dollar, Häuser und Grundstücke. Auch andere regimetreue Medien in Marokko bezeichnen den Aktivisten seit Jahren als Dieb, Geldwäscher, Verräter oder Homosexuellen, diffamieren und beleidigen ihn. Seit bald einem Jahrzehnt trotzt Maati Monjib dem Diffamierungs- und Überwachungsdruck – und zahlt einen hohen Preis dafür.

O-Ton Maati Monjib, darüber Übersetzung:

Mindestens einmal die Woche breche ich in Tränen aus – aus purer Verzweiflung. Das Regime verfolgt mich, obwohl ich mein Land liebe und auch die Regierung nicht stürzen will. Ich verteidige nur die Menschenrechte der Marokkaner. Und wegen der ständigen Drohungen und Verleumdungen musste ich meine 16-jährige Tochter ins Ausland schicken. Trotzdem: Ich werde durchhalten. Nein, aufgeben werde ich mit Sicherheit nicht.

Autor:
Am 29. Dezember 2020, wenige Tage nach unserem Gespräch, wird Maati Monjib in Rabat festgenommen und angeklagt wegen Betrugs und „Untergrabung der Staatssicherheit“. Am 28. Januar 2021 wird er verurteilt – zu einem Jahr Haft ohne Bewährung.

Musikakzent

Autor:
Zum Glück seien Menschenrechtler nicht völlig wehrlos gegenüber staatlicher Überwachung, sagt der deutsche Aktivist Peter Steudtner. Hundert Tage saß Steudtner in einem türkischen Gefängnis, weil er Nicht-Regierungs-Organisationen der Zivilgesellschaft zu Fragen der Datensicherheit beraten hatte: Wie können sie sich, ihre Kontakte, ihre Daten schützen vor staatlicher Überwachung? Doch für türkische Behörden grenzt es schon an Terrorismus, Organisationen dabei zu beraten, wie sie sensible Daten möglichst sicher verschlüsseln.

Ein anderes Mittel, staatliche Überwachung zu unterlaufen, sind virtuelle private Netzwerke, sogenannte *VPN-Tunnel*. Mit ihnen kann man sich im Internet tarnen, weil nicht mehr erkennbar ist, wo man gerade ist.

O-Ton Peter Steudtner:
Mit so einem Tunnel kann man sich in ein anderes Land hinein versetzen. Das heißt, meine Internetverbindung geht hier in einen Tunnel hinein und kommt dann meinetwegen in Niederlanden, in den USA, wo auch immer, wieder raus. Und dort hat man dann Zugang zu den Inhalten. Für die Menschenrechtsarbeit nutzen diese VPN-Tunnel auch, weil man damit die Daten schützen kann vor den Eingriffen der jeweiligen Regierung.

Autor:
Wenn die Regierung nicht ihrerseits Technologie erworben hat, die solche VPN-Tunnel blockt – oder auch den Zugang zu sicheren Messenger-Diensten wie Signal und Threema.

Musikakzent

Autor:
Der Export von Überwachungstechnologie aus der EU in autoritär regierte Länder müsse radikal begrenzt und viel besser kontrolliert werden, meint Lena Rohrbach von *Amnesty*. Auf weltweite Regelungen zu warten, sei sinnlos. Und das *Wassenaar-Abkommen*, das den Handel mit *dual use*-Gütern regelt, komme der rasanten Entwicklung gerade bei der Überwachungstechnik überhaupt nicht hinterher.

O-Ton Lena Rohrbach:
Im *Wassenaar-Abkommen* sind über 40 Staaten Mitglied und das ist eine sehr unterschiedliche Gruppe. Da sind die EU-Staaten dabei, auch USA, Russland oder die Türkei beispielsweise. Und da kann man sich schon vorstellen: Wenn sich also die USA, Russland und die Türkei mit ihren jeweils unterschiedlichen Interessen auf eine Liste der Exportkontrolle einigen müssen, das ist sehr schwer und folglich ist diese Liste auch eher minimalistisch. Das heißt: Viele Güter fehlen da. Zum Beispiel biometrische Überwachung wie Gesichtserkennung steht da nicht mit drauf. Systeme der Vorratsdatenspeicherung stehen da nicht mit drauf. Und um etwas neu aufzunehmen, das dauert sehr lange.

Autor:
Nach langem Drängen von Menschenrechtsorganisationen und Europaparlament machte die EU-Kommission 2016 einen Vorstoß, die *dual use*-Verordnung der EU grundlegend zu reformieren. Vier Jahre stritten anschließend die Mitgliedsstaaten; sie verteidigten Souveränitätsrechte und Wirtschaftsinteressen; etliche Staaten wollten um keinen Preis ihre Entscheidungsmacht über Exportkontrolle abtreten an die EU. Das müsse man verstehen, meint Stéphane Chardon, der leitende Exportkontrolleur der EU-Kommission.

O-Ton Stéphane Chardon, darüber Übersetzung:
Der Vorschlag der EU-Kommission von 2016 markiert einen grundlegenden Wandel: Anders als bisher nämlich soll künftig die EU Leitplanken setzen für die europäische Exportkontrolle. Vor diesem Schritt schreckten etliche Staaten jahrelang zurück. Sie wollten weiter selbst entscheiden. Und eine starke Minderheit von Staaten blockierte den grundlegenden Beschluss, die EU zu einem wichtigen Akteur zu machen bei der Exportkontrolle.

Autor:
Im November 2020 einigten sich die Mitgliedsstaaten schließlich; noch vor dem Sommer 2021 soll die reformierte *dual-use*-Verordnung in Kraft treten. Geplant ist eine von globalen Abkommen unabhängige *watchlist* der EU. Diese Beobachtungsliste soll menschenrechtlich problematische Güter enthalten – und problematische Adressaten für den Export solcher Güter. Sie ist allerdings höchst unverbindlich: Damit ein Gut überhaupt gelistet wird, muss zunächst ein EU-Staat Exportkontrollen dafür einführen. Und nur wenn dann kein anderer Staat widerspricht, kommt das Produkt auf die *watchlist*.

Hinzu kommt: Selbst wenn eine Überwachungstechnologie auf die EU-Kontrollliste kommt, entscheidet, immer noch jedes einzelne Land, ob es eine Exportgenehmigung erteilt oder nicht.

Musikakzent

Autor:
Die neue EU-*watchlist* soll, immerhin, möglichst schnell auch neu entstehende Technologien erfassen. Und die Hersteller sollen eingebunden werden. Sie kennen ihre Technologie schließlich am besten und könnten mithelfen, Missbrauch, also Menschenrechtsverletzungen, zu vermeiden – meint Lena Rohrbach.

O-Ton Lena Rohrbach:
Wir haben also gefordert, dass Unternehmen auch sogenannte menschenrechtliche Sorgfaltspflichten bekommen. Das heißt, dass sie ihre geplanten Exporte auch selbst darauf überprüfen müssen, ob die möglicherweise zu Menschenrechtsverletzungen beitragen könnten und dann gegebenenfalls vorsichtshalber eine Lizenz, eine Genehmigung bei der nationalen Ausfuhrbehörde erbitten, wenn sie da ein Risiko sehen – auch dann, wenn die Technik eigentlich gar nicht auf der Liste steht.

Autor:
Nein, entgegnet Nikolas Keßels, Referent für Außenwirtschaftspolitik beim *Bundesverband der Deutschen Industrie*, *BDI*. So gehe das nicht. Industriemanager könnten sich nicht aufs Glatteis eigener Einschätzungen von Menschenrechtsfragen begeben. Sie bräuchten juristisch klare Regeln und Listen.

O-Ton Nikolas Keßels:
Im deutschen Ausfuhrkontrollrecht gibt es ordnungs- und strafrechtliche Konsequenzen bei Verstößen, die Gefängnisstrafen von bis zu 15 Jahren nach sich ziehen. Rechtsklarheit, gerichtsfeste Entscheidungen sind da für die Unternehmen das A und O. Wenn die nicht bestehen, dann ist die Konsequenz, dass für alles, was irgendwie auch nur entfernt in die Wurfweite einer solchen Fragestellung gerät, beantragt wird. Dafür hat niemand die Ressourcen, geschweige denn die Zeit.

Autor:
Die künftige Verordnung sieht nun vor, dass Exporteure von Überwachungstechnik menschenrechtliche Aspekte zwar prüfen sollen. Eine Exportgenehmigung beantragen aber müssen sie nur, wenn sie sich bewusst sind oder Informationen darüber haben, dass die Technik zur Verletzung von Menschenrechten genutzt werden soll. Wenn dies nur theoretisch möglich oder auch wahrscheinlich ist, aber keine konkreten Hinweise vorliegen, müssen sie keine Genehmigung beantragen. Der Entwurf der neuen EU-*dual-use*-Verordnung umfasst mehrere hundert Seiten. Und er enthält weitere Formulierungen, die Zweifel aufkommen lassen, ob diese Verordnung in der Praxis viel verändert. Artikel 1.21, zum Beispiel, definiert, für welche Überwachungstechnologie die neue Export-Verordnung regelt:

Zitat Verordnungsentwurf:
Gegenstände zur Internet-Überwachung sind zivil und militärisch nutzbare Gegenstände, die speziell dafür entwickelt wurden, die verdeckte Überwachung natürlicher Personen zu ermöglichen.

Autor:
Diese Definition habe die Industrie durchgesetzt, meint Lena Rohrbach:

O-Ton Lena Rohrbach:
Das bedeutet, dass künftig nur Technologie genehmigungspflichtig gemacht werden kann, die verdeckt überwacht. Und es gibt aber eben ganz besonders im Bereich der öffentlichen Videoüberwachung auch Technologie, die bekanntermaßen öffentlich überwacht und die trotzdem nicht weniger problematisch ist, sondern gerade zu Kontrollen ganzer Bevölkerungen genutzt werden kann.

Autor:

Videokameras, zum Beispiel; Software zur Gesichtserkennung und Emotionsanalyse würden nach dieser Definition schon mal aus der Kontrolle rausfallen. Außer in einem speziellen Fall: Werden mit der offen überwachenden Technik unbestreitbar schwere Menschenrechtsverletzungen in einem Land begangen, kann die Ausfuhr in dieses Land doch der Genehmigungspflicht unterworfen werden. Ein mögliches Beispiel: der Export von Gesichtserkennungstechnologie nach China. Er könnte möglicherweise gebremst werden.

Musikakzent

Atmo:
Werbespot von CEPOL

Autor:
CEPOL, die *Europäische Polizeiakademie* mit Hauptquartier in Budapest. *CEPOL* bildet EU-Polizisten aus, schult jedoch auch – im EU-Auftrag – Sicherheitskräfte in autoritär regierten Ländern. Sie lernen von deutschen, österreichischen oder spanischen Polizisten, wie man Menschen, Organisationen und die Bevölkerung eines ganzen Landes überwacht. Dies dokumentiert die britische Menschenrechtsorganisation *Privacy International* in einem Ende 2020 vorgelegten Bericht.

O-Ton Edin Omanovic, darüber Übersetzung:
In unserem Bericht dokumentieren wir, wie Agenten der *EU-Polizeiakademie* Sicherheitskräfte in Nordafrika und auf dem Balkan ausbilden beim Umgang mit Überwachungstechnik. Zu den Ausbildungsinhalten zählt das Ausspähen von Nutzern sozialer Medien – in krassem Widerspruch zu den Richtlinien der Medienplattformen.

Autor:
Die aufgedeckten Vorgänge konterkarierten sämtliche EU-Bemühungen um die Begrenzung kommerzieller Überwachungsexporte, meint der verantwortliche Mitarbeiter der Organisation Edin Omanovic:

O-Ton Edin Omanovic, darüber Übersetzung:
Die EU liefert zudem den Grenzschutzbehörden der betreffenden Länder modernste Überwachungstechnik; Systeme biometrischer Massenüberwachung, zum Beispiel, die die Daten von Millionen Menschen speichern können. So kann die EU den Schutz ihrer Außengrenzen vor Migranten outsourcen – finanziert mit Geld, das eigentlich für Entwicklungshilfe bestimmt ist. In einem Dokument ist auch von einem Austausch von Überwachungsdaten die Rede, um die Deportation illegaler Migranten zu erleichtern.

Autor:
Kampf gegen Terrorismus, Kampf gegen illegale Migration. So rechtfertigt es die EU, dass EU-Polizisten Sicherheitskräften diktatorisch regierter Staaten helfen, ihre Bevölkerung zu überwachen. Massenhafte Erhebung, Verarbeitung und der Austausch persönlicher Daten von Nicht-EU-Bürgern zählen ausdrücklich zum Konzept.

Die Menschenrechtsorganisation *Privacy International* hatte Gelegenheit, Kursunterlagen für diese Schulungen einzusehen. Sie dokumentieren, wie Algeriens Gendarmerie von EU-Polizisten lernt, wie sie soziale Medien überwachen kann; wie sie *Fake*-Profile anlegen sowie Smartphones lokalisieren und *hacken* kann. Algerien ist bekannt dafür, dass es aus dem südlichen Nachbarland Niger kommende Migranten mit brachialen Methoden deportiert. Zahlreiche Journalisten und Oppositionelle sitzen in algerischen Gefängnissen.

Ähnlich in Tunesien. Dort enthalten die Schulungsunterlagen der Europäischen Polizeiakademie Hinweise, wie man die Finanzquellen zivilgesellschaftlicher Organisationen aufgedeckt. Und sie suggerieren geradezu, dass solche Organisationen Geld vor allem für terroristische Zwecke sammeln würden.
Das Europäische Parlament wisse wenig über Aktivitäten der Polizeiakademie *CEPOL* außerhalb des EU-Territoriums, berichtet Paul Diegel. Der Politikwissenschaftler berät das Parlament zum Thema Überwachungsexporte.

O-Ton Paul Diegel:
Wir haben eine offizielle Frage an die Kommission gestellt, was *CEPOL* gemacht hat, was die Serviceleistung war und wie das mit unserem human rights und *regional stability* und *security approach* zusammenhängt. Also die Befürchtung hier ist, dass man marokkanischen oder libyschen oder algerischen Sicherheitskräften nicht nur das Knowhow gegeben hat, sondern auch tatsächlich anscheinend gesagt hat, welche Produkte man denn am besten kaufen sollte, um Leute zu überwachen.

Autor:
Damit nicht genug: Bezahlt wird die EU-Polizeihilfe für autoritär regierte Staaten unter anderem aus einem gut ausgestatteten EU-Finanztopf mit dem wohlklingenden Namen: *EU Trust Fund for Africa*. Ein Fonds, der eigentlich dafür gedacht ist, mit Entwicklungshilfe die Ursachen von Terrorismus und illegaler Migration zu bekämpfen. Stéphane Chardon von der EU-Kommission zeigt sich eher schmallippig bei diesem Thema.

O-Ton Stéphane Chardon, darüber Übersetzung:
Ich kann zu Einzelheiten dieser Vorgänge leider keine Stellungnahme abgeben. Grundsätzlich sagen kann ich aber: Eine Zusammenarbeit der EU oder eines Mitgliedsstaats mit bestimmten Ländern verkörpert wahrscheinlich den besten Weg, die Behörden dort zu sensibilisieren für den angemessenen Umgang mit Überwachungstechnik.

Autor:
Wie beim kommerziellen Export von Überwachungstechnologie setze die EU mit ihrer Überwachungshilfe für autoritäre Regime ihre Glaubwürdigkeit aufs Spiel, resümiert Edin Omanovic von *Privacy International*. Wer derart zynisch mit den Menschenrechten jenseits der eigenen Grenzen umgehe, verliere das Vertrauen auch der eigenen Bürger.

O-Ton Edin Omanovic, darüber Übersetzung:
Die EU spielt eine sehr wichtige Rolle bei der Förderung von Menschenrechten und Demokratie, beim Schutz auch von Journalisten und der Zivilgesellschaft weltweit. Und ich finde, die EU sollte sich endlich der grundsätzlichen Frage stellen, ob sie die

Sicherheit von Diktatoren und Staaten schützen will oder die Sicherheit von Menschen.

Musikakzent

Autor:
Ernüchterndes Fazit: Das Verhalten der EU in Sachen "Überwachungstechnik für Diktatoren“ bleibt geprägt von Widersprüchen, Inkonsequenz und mangelnder Glaubwürdigkeit. Daran dürfte die neue *dual-use*-Verordnung wenig ändern. Die EU ist da allerdings keine Ausnahme: Auch andere Staaten kontrollieren den Export von Überwachungstechnologie kaum, klagt Lisa Dittmer, Sprecherin der Organisation *Reporter ohne Grenzen*.

Musikakzent

O-Ton Lisa Dittmer:
Letztlich braucht es natürlich über die EU hinaus effektive Exportregime. Ganz klar ist, dass auch Länder wie die USA und Israel große Produzenten von digitaler Überwachungstechnologie sind und diese bislang viel zu wenig diskriminierend in zahlreiche Staaten liefern. Ich glaube, die EU trägt eine gewisse Verantwortung, jetzt voranzugehen und zu sagen: „Wir wollen eben eine wertebasierte Ausfuhrkontrolle.“ Aber effektiv kann man all diesen Handel nur einschränken, wenn man auf internationaler Ebene sich einigt.

Autor:
Der Weg zu internationalen Vereinbarungen in Sicherheitsfragen jedoch ist lang, mühsam und steinig. Das haben schon die zähen Verhandlungen innerhalb der EU gezeigt.

*****