Herausgegeben von
Marlene Straub

Privatsphäre

9// *20 Jahre später*

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

DOI: 10.17176/20230215-144904-0

Verfassungsblog gGmbH
Großbeerenstr. 88/89
10963 Berlin
www.verfassungsblog.de
info@verfassungsblog.de

Umschlaggestaltung Carl Brandt

Diese Publikation wurde im Rahmen des Fördervorhabens 16TOA045 mit Mitteln des Bundesministeriums für Bildung und Forschung erarbeitet und im Open Access bereitgestellt.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Die Blog-Symposien wurden im Zuge des Modellprojektes „20 Jahre 9/11“ durch die Bundeszentrale für politische Bildung gefördert.

Gefördert durch die bpb: Bundeszentrale für politische Bildung

Marlene Straub (Hrsg.)

Privatsphäre

9/11, 20 Jahre später: eine verfassungsrechtliche Spurensuche

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

Vorwort

Auf der ganzen Welt haben Staaten nach den Anschlägen vom 11. September 2001 die nationale Überwachung und internationale Überwachung ausgeweitet. Die massiven Verletzungen des Rechts auf Privatsphäre, die damit einhergehen sind vor allem mit den Enthüllungen von Edward Snowden in das öffentliche Bewusstsein gerückt. Sie lösten zwar große Empörung aus, doch die Strukturen, die diese Überwachung ermöglichen, bleiben weitgehend bestehen. Tatsächlich scheinen sich Staaten bei der Überwachung privater Kommunikation gegenseitig überbieten zu wollen und weiten die Befugnisse ihrer Nachrichtendienste trotz grund- und menschenrechtlicher Bedenken weiter aus. Die Terrorismusbekämpfung und die nationale Sicherheit dienen dem allen als Rechtfertigung.

In diesem Symposium befassen sich die Autor*innen mit der Normalisierung der Überwachung und den allgegenwärtigen Eingriffen in die Privatsphäre seit 9/11. Es geht um den totalitären chinesischen Überwachungsstaat und darum, wie die indische Regierung sich davon inspirieren lässt, während amerikanische Polizist*innen auf sozialen Medien Fake-Accounts zur Überwachung nutzen. Im Europäischen Kontext scheinen Gerichte auf EU- und mitgliedstaatlicher Ebene die wahllose Überwachung zu normalisieren, wenn sie ihr nicht sogar durch ihre Rechtsprechung den Weg ebnen. Wir erfahren, wie illiberale europäische Demokratien

Überwachungsbefugnisse missbrauchen und dass sich nicht annähernd quantifizieren lässt, in welchem Umfang sich die „Überwachungslast" in Europa seit 9/11 tatsächlich verändert hat. Dieses Symposium zeichnet das pessimistische Bild einer Negativspirale in Rechtsprechung und Gesetzgebung – es zeigt aber auch, dass sich in allen untersuchten Ländern und Regionen organisierter Widerstand gegen die ungezügelte Überwachung wehrt.

Dieses Buch mit 11 Beiträgen ist nach dem Band „9/11, Menschenwürde und die liberalen Grundwerte" der sechste in einer Reihe von sieben Bänden. Diese Buchreihe ist aus zwei Projekten des Verfassungsblogs hervorgegangen: Gefördert von der Bundeszentrale für Politische Bildung konnten wir im Rahmen des *Projekts 9/11, 20 Jahre später: eine verfassungsrechtliche Spurensuche* sieben Blog-Symposien realisieren. Unser vom Bundesministerium für Bildung und Forschung gefördertes Projekts *Offener Zugang zu Öffentlichem Recht* hat uns ermöglicht, aus diesen Symposium Bücher zu machen. Dabei wollen wir den digitalen Ursprung dieses Buches nicht leugnen: mit dem QR-Code auf der rechten Seite gelangen Leser*innen direkt zum Blog-Symposium, und über die einzelnen QR- Codes, die den Beiträgen vorangestellt sind, zu den einzelnen Texten – eine Idee, die wir uns bei den Kolleg*innen vom Theorieblog abgeguckt haben. Über diesen kleinen Umweg lassen sich die Quellen nachvollziehen, die in der Printversion an den ur-

sprünglich verlinkten Stellen grau gehalten sind.

Marlene Straub

Inhalt

Albert Fox Cahn and Nina Loshkajian

On the Internet, No One Knows You're a Cop

Police and Social Media Deception

Across America, police are using an expansive new power to access private social media content, viewing some of our most intimate moments, with absolutely no judicial oversight. This power isn't some unreported provision of the USA PATRIOT Act, it's not some shadowy executive order. No, the authorisation for this sprawling surveillance apparatus is just 3 words long: "Accept friend request". Increasingly, internet surveillance is operating under our consent, as police harness new software platforms to deploy networks of fake accounts, tricking the public into giving up what few privacy protections the law affords. The police can see far beyond what we know is public on these platforms, peaking behind the curtains at what we mean to show and say only to those closest to us. But none of us knows these requests come from the police, none of us truly consent to this new, invasive form of state surveillance, but this "consent" is enough for the law, enough for the courts, and enough to have our private conversations used against us in a court of law.

Police use of fake social media accounts

COVID-19 only accelerated our growing reliance on social media and internet platforms, finding digital community amid the constant separation. Our increased reliance on digital platforms has created an increased risk of police surveillance, particularly for young Black and Brown Americans.

"Anti-gang" policing has driven officers to scrutinise targets' every Instagram selfie and TikTok clip as a potential clue or even a confession. But while police can and do scour public social media accounts with abandon, they need court approval to access private accounts, that is, unless they have our "consent."

To obtain it, officers don't simply stroll up and ask if we'd like to be targets of a police investigation. Instead, they increasingly turn to internet attribution software or technology sold by private vendors to deploy large numbers of fake credentials. One police officer can run a bot network of hundreds or thousands of fake accounts. These accounts are used to harvest private messages and posts for local police databases. Private vendors of social media monitoring software tout their ability to allow bulk creation of undercover accounts and to store unlimited numbers of them in databases.

Private vendors are enabling the deception, selling spying technology to police departments. The LAPD pursued a contract with Voyager Labs to use a software product that allowed them to conduct undercover monitoring using fake social media profiles. As documented by the Brennan Center for Justice, the software surveils more than just the suspect, but also collects data on everyone they know on the platform. These sprawling networks of surveillance are deemed permissible based on the "consent" given by only the sin-

gle individual who accepts a request from an officer's fake account, a remarkably tenuous basis.

Replicating the harmful patterns of undercover policing

Police use this deceit to replicate the federal government's bulk data collection programs, mapping out networks of people based on their political and religious beliefs.

This new form of deceptive policing is a digital version of the infiltration of Muslim communities in the post-9/11 era. For more than a decade, undercover officers and informants systemically targeted Muslim New Yorkers for simply practising their faith, attempting to monitor conversations that took place in mosques, Muslim-owned businesses, religious schools, and community groups. While this program failed to generate even a single credible lead, it sent a clear message to Muslim New Yorkers that their conversations would be watched. Through fake social media accounts, police can replicate this infiltration for online communication, monitoring Facebook groups, WhatsApp chats, and other digital community spaces. Just because this activity is taking place online, it does not make it any less intimate and sensitive, and certainly does not erode the First Amendment interests at stake.

Voyager Labs claims to perceive people's motives and identify those "most engaged in their hearts" about their ideologies. As part of their marketing materials, they touted

retrospective analysis they claimed could have predicted criminal activity before it took place based on social media monitoring. However, the case studies reveal monitoring tools that are designed to profile users for the faith they practice today, not for crimes they might commit tomorrow. Much of the content flagged shows nothing more than the fact that the targets practice Islam or are of Arab descent.

In Memphis, Tennessee, police used multiple fake Facebook accounts to surveil Black Lives Matter activists, accessing private posts and even cataloguing the names of people who had "liked" those posts. The disturbing practice only came to light after activists were arrested, leading Facebook to urge the department to stop the practice.

Police systematically target youth, stifling their ability to engage with the digital communities that we take for granted. Children and teens are increasingly weary of the presence of police online, often self-censoring communications to avoid the danger of being swept up in these digital dragnets. They enjoy a First Amendment right to unfettered internet communications in theory, but they face a very different reality in practice.

Protecting our private communications

As long as police can continue to exploit the legal fiction of user "consent" to access our private communications, our

privacy rights will remain just as fictional. While we're hopeful that the courts will one-day strike this practice down as violating the Fourth Amendment, more urgent statutory protections are needed. The legislation needn't be lengthy or complex, it's not a nuanced question. To the contrary, what we need is a complete and categorical ban on the use of fake accounts by police, letting those who've been surveilled sue, and suppressing the evidence that's obtained at trial. The practices have thus far evaded public scrutiny, with departments refusing to disclose the number of fake accounts they maintain. Left unchecked, this threat to our private communications will only grow. As more of our lives move onto digital platforms, as our real world becomes ever more displaced by augmented and virtual realities, the vaunted rise of the metaverse, much more of what we say will be susceptible to police tracking through these tactics. Yes, we can train the public to be more sceptical of granting consent, yes tech platforms can make it harder for police, but ultimately, none of these steps are a substitute for robust privacy protections that can't simply be clicked away.

Maria Tzanou

Public Surveillance before the European Courts

Progressive Legitimisation or a Shift Towards a More Pragmatic Approach?

Following 9/11 and the subsequent terrorist attacks on European soil, a significant expansion of state surveillance, counter-terrorism regimes in Europe and worldwide has taken place. While such regimes demonstrated the increasing appetite of law-makers and the executive for normalisation of surveillance, at the same time, a significant development towards the opposite direction started to emerge from the two main European Courts – the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR): a powerful pushback against the normalisation of state surveillance. This pushback coming from the judiciary has produced several celebrated victories for fundamental rights over surveillance. Indeed, the jurisprudence of the CJEU was seen as initiating a progressive trend, marking continuous victories of EU fundamental rights against not only the EU legislature but also Member States' policymakers and even third countries' surveillance regimes, such as the USA.

However, the recent decisions by the CJEU in *La Quadrature du Net* and the ECtHR in *Big Brother Watch and Others v. the UK* reveal a different picture: both Courts are now moving towards the legitimisation of surveillance in the public sphere. Does this mean that the progressive trend that emerged after 9/11 has reached its limits? More importantly, are European courts now normalising surveillance? This post unpacks the implications of this new judicial trend

by addressing the above questions. I argue that such a trend – properly circumscribed – might signify a less naïve approach to surveillance.

The CJEU data retention "saga"

The CJEU has delivered a series of landmark decisions on state surveillance measures. This expansive jurisprudence commenced in 2014 with *Digital Rights Ireland*, where the CJEU invalidated the *Data Retention Directive* ruling that indiscriminate bulk metadata retention is incompatible with EU law. It continued in 2015 with *Schrems I*, in which the Court found that the US authorities' access to personal data transferred from EU Member States under the Safe Harbour scheme went beyond what was strictly necessary and proportionate to the protection of national security. It further culminated in 2017 with *Tele2 and Watson*, where the Court held that the *Digital Rights Ireland* principles applied to national laws implementing the invalidated Data Retention Directive. It continued in 2018 with Ministerio Fiscal, in which the CJEU clarified that different types of data retention measures entail different levels of interference with fundamental rights. In *Schrems II*, delivered in 2020, the Court annulled the Privacy Shield adequacy decision holding that US national security requirements cannot be given primacy over EU data protection principles. Finally, in *Privacy International*, the CJEU reiterated that indiscriminate bulk reten-

tion is prohibited, even when this is undertaken for national security purposes.

This long line of cases shows what I consider a trend of judicial pushback against the normalisation of surveillance. The judgments of the CJEU are far from perfect (I have criticised different aspects of them, here and here), but they do establish clear red lines of what is considered prohibited public surveillance.

La Quadrature du Net and Big Brother Watch: A judicial shift?

The *La Quadrature du Net* judgment was rendered on the same day as *Privacy International*. But, while the latter continues the CJEU's expansive data protection jurisprudence, *La Quadrature du Net* marked an important departure from the Court's prohibitive approach to bulk data retention to a more nuanced one that cracks the door open for a variety of different permissible surveillance measures, if these are carried out under certain criteria and applicable safeguards. Indeed, the most important contribution of *La Quadrature du Net* was the establishment of a long list of permissible data retention measures that paints a comprehensive but complex picture of acceptable law enforcement tools and makes several major concessions to Member States' security authorities – including allowing for general, indiscriminate preventive data retention when confronted with a "serious"

threat to national security "which is shown to be genuine and present or foreseeable".

A similar trend is evident in the jurisprudence of the ECtHR. For instance, in *Big Brother Watch* and *Centrum för Rättvisa v. Sweden* delivered in May 2021, the starting point of the Grand Chamber of the ECtHR's analysis was that bulk interception regimes are "a valuable technological capacity to identify new threats in the digital domain". The ECtHR also opted for a more nuanced approach to bulk surveillance, prescribed by several procedural guarantees regarding authorisation, retention, access and oversight. In particular, the Grand Chamber set out several so-called "end-to-end safeguards" that provide adequate and effective guarantees against arbitrariness and abuse. More recently, in *Ekimdzhiev and others v. Bulgaria*, the ECtHR continued along these lines, emphasising that such procedures should not only exist on paper, they should also operate in practice.

A judicial normalization of surveillance or a more pragmatic approach?

These guarantees, conditions and safeguards demonstrate a more proceduralised approach to surveillance. They also signal backtracking from red lines (in particular, regarding the prohibition of bulk surveillance), towards a gradual acceptance. This new approach might be good news for na-

tional governments as it presents relatively "easy fixes" to the inherent problems of bulk data retention.

However, in the words of Judge Pinto De Albuquerque it also "fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests" by progressively re-legitimising bulk data retention on the condition that effective guarantees are applicable. In this respect, it is hard to agree with his argument that "the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe". Instead, it seems that the two Courts are converging rather than diverging in their recent jurisprudence concerning the data retention saga.

Moreover, the list of permissible surveillance measures laid down by the CJEU in *La Quadrature du Net* is so prescriptive that the Court seems to be assuming a *quasi-legislative* role. Indeed, it appears to expand its assessment of data retention both *vertically* (entering the Member States' realm) and *horizontally* (entering the legislator's realm). At first glance, one could criticise the CJEU for overstepping its boundaries. However, a deeper analysis reveals the complexity of the questions that underpin metadata surveillance: If data retention cannot be harmonised at the EU level, then how would EU fundamental rights be ensured at the national level where data retention measures are fragmented and vary between different Member States? Would

a more *laissez-faire* approach not be equally problematic for both fundamental rights and overall legal certainty concerns?

It seems, therefore, that a more pragmatic judicial approach to surveillance might be needed. This might be interpreted by some as opening the path towards a normalisation of surveillance. However, I argue that we should be cautious here, especially under the current political circumstances that find Europe at a turning point in its history after the Russian military invasion of Ukraine. It would be naive to criticise the European Courts for adopting a more proceduralised approach to surveillance based on conditions and safeguards rather than prohibitive red lines. Such an approach might also present less risk to the Courts finding their judgments circumvented – or altogether ignored by the executive.

Conclusion

A new judicial trend can be observed that marks the beginning of a more nuanced approach to surveillance that opens the door for bulk data retention measures when these are required for counter-terrorism purposes.

This re-evaluation of data retention models seems to be based on what this post referred to as the "proceduralization of surveillance". Instead of red lines and prohibitive rules, data retention measures are now gradually permitted

on the basis of a set of procedures, criteria, and safeguards under which they should operate. This is a significant departure from the previous case law that signals a progressive re-alignment of the CJEU with the ECtHR.

Overall, Courts do not have an easy task when attempting to find a compromise between law enforcement and intelligence services' requirements and fundamental rights. It often happens that their judgments anger both national governments and privacy advocates equally. The future will show whether the progressive re-legitimisation of public surveillance through its circumcision under conditions, safeguards and oversight will open the gates for an electronic "Big Brother" in Europe, or lead the way towards a less absolute, more pragmatic (and perhaps less naïve) approach to surveillance. What is for sure is that the data retention saga is not over yet.

Eliza Watt

The Legacy of the Privacy versus Security Narrative in the ECtHR's Jurisprudence

In this post I trace the modern culture of mass surveillance to the UN policy of counterterrorism resulting from the 9/11 attacks on the United States. I argue that balancing security needs with privacy rights on the basis of the traditional security/privacy trade-off is misguided, and identify the complexities involved in the modern culture of surveillance. Further, I highlight that the security narrative has always played an important role in the European Court of Human Rights' (ECtHR) law-making, ultimately leading to the Court's embracing of mass surveillance practices.

Privacy vs security: The misguided trade-off

One of the inevitable consequences of the 9/11 UN counterterrorism policy is a "surveillance industrial complex" fuelled by heightened threat narrative, initially presented by some governments as a trade-off. Accordingly, security can only be achieved if it is accepted that states must conduct mass surveillance in order to keep their citizens safe. While this means sacrificing their fundamental rights-the argument goes-this is the price to be paid for attaining greater safety for all. Most importantly this means compromising the right to privacy, being "the presumption that individuals should have an area of autonomous development, interaction and liberty free from State intervention and excessive unsolicited intrusion by other uninvited individuals".

The two decades of counterterrorism strategy that followed attest to the fact that the security/privacy trade-off approach is not only outdated, but it also amounts to a gross oversimplification of the complexities involved in the modern culture of surveillance. First, it has been contended that the threat of terrorism has at times been sensationalised owing to deliberately engineered "politics of fear". This arguably resulted in the UN prioritising, magnifying and overestimating terror-related risks over other existential threats to international peace and security, thus consequently diverting resources and attention from other pressing issues, such as climate change or deadly pandemics. To illustrate this, in statistical terms the estimated number of deaths in 2021 from the Covid-19 pandemic was reported to reach 1,884,146 compared with 7,142 deaths recorded due to global terrorism. Secondly, the traditionally defined trade-off discounts the "public-private symbiosis", which sees data as a commodity to be exploited for commercial gains through state-business partnerships. It follows that spying and surveillance can no longer be perceived as purely pursued for political or economic ends between nation-states or explained solely as a national security necessity. Commercial spying, known as "surveillance capitalism", by private companies in the form of consistent monitoring, predicting and influencing consumer behaviour on the internet is now habitually carried out for profit and often merges and col-

laborates with state surveillance, forming a global "surveillance industry".

One example is the 2021 Pegasus scandal, software sold worldwide by the Israeli NSO Group to governments, including within the European Union (EU), to spy on a coterie of world leaders, politicians, human rights activists and journalists rationalised inter alia by the need to fight terrorism. As Amnesty International put it, this case is emblematic of the private sector facilitating surveillance, of impunity of states and companies in deploying it, together with the failure of the former to fulfil their obligations to protect individuals from unlawful hacking and surveillance.

Of equal importance in this emergent paradigm is the role of individuals, who often voluntarily surrender their privacy by publicly sharing their data on social media platforms such as Instagram, YouTube, or Twitter. This phenomenon is termed "participatory panopticon" and described as "constant surveillance [which] is done by citizens themselves, and [which] is done by choice". For these reasons alone, presenting the problem of reconciling security needs with privacy rights as a "trade-off" is misplaced. Democracies depend on data as a commodity and spying related to national security apparatus is but one manifestation of a new culture of persistent surveillance, which is here to stay. Rather than a trade-off, it must be redefined in terms of cost-benefit analysis. This means the estimate of the real cost to privacy

and related human rights associated with mass surveillance whilst not attaining security to the degree advocated by governments, and fully recognising the resultant commercial gains made by governments and the private sector alike.

ECtHR jurisprudence on mass surveillance post-Snowden disclosures

The post-9/11 culture of mass surveillance has been subject to extensive and fierce debate, especially in the years that followed the revelations made by Edward Snowden in 2013. Strict legal scrutiny, in particular by the European Court of Human Rights, has played a significant role in this discourse. This is because in its mass surveillance case law the Court addresses states' arbitrary interference with the right to privacy set out in Article 8 of the European Convention of Human Rights (ECHR), which national authorities have often justified on national security/terrorism grounds.

In a number of important cases, including *Roman Zakharov v Russia, Centrum för Rättvisa v Sweden* and *Big Brother Watch and Others v United Kingdom,* the ECtHR has remarkably adjusted its jurisprudence, in some instances rejecting well-settled principles upon which it had previously relied. Two issues vividly illustrate this unprecedented transformation, namely the Court's approach to the right to bring an individual complaint (the so-called 'victim status') and its acceptance of mass surveillance programmes *per se*.

The right to bring a claim before the ECtHR in surveillance cases

Under Article 34 of the ECHR, the ECtHR may hear applications from an individual, non-governmental organisation or group claiming to be a victim of a violation of any of the ECHR rights by any of its contracting state parties. For the best part of six decades, the Court consistently interpreted this provision as requiring the applicant to evidence that he or she was personally and directly a victim of violation and, more recently, that he/she suffered a "significant disadvantage". If these criteria were not satisfied, the Court would not review the member state's law or policy *in abstracto*, that is in the absence of any evidence as to how his/her privacy was actually violated. This changed significantly in 2015 as a result of *Zakharov v Russia*. In this case the Court recognized that individuals would not normally be aware of being the subject of secret surveillance and allowing cases to be brought even where the claimant cannot prove that they were the subject of a concrete surveillance measure. By allowing an individual to claim to be a victim of a state's violation on the basis of the mere existence of secret surveillance methods, or of legislation permitting their operation provided that he/she can show to potentially be at risk of being subjected to them, the ECtHR was able to scrutinise state clandestine surveillance in Europe ever since.

The key outcomes of this striking change are the landmark cases of *Big Brother Watch* and *Centrum för Rättvisa,*

issued in parallel, both concerning bulk interception of foreign communications by the United Kingdom and Sweden respectively. For two reasons the judgements are of vital importance for the future of the Council of Europe (CoE) states' spying policies. First, the ECtHR has explicitly recognised mass surveillance regimes as not *ipso jure* incompatible with Convention rights. In contrast, the Court of Justice of the European Union (CJEU) in a number of high-profile cases held that blanket retention and data sharing arrangements with third countries are incompatible with the EU citizens' rights to privacy and data protection. The CJEU reaffirmed this stance in early April 2022 in *Commissioner of An Garda Síochána and Others*. It held that as a general principle, EU law does not allow for legislation that as a preventative measure permits general and indiscriminate retention of traffic and location data for the purposes of combating serious crime, but it does not preclude member states' targeted and time-limited legislative data retention measures.

Secondly, the ECtHR recognised the challenges states face with fighting serious crime and international terrorism brought about by the changes in technology and communications. It, therefore, updated the procedural safeguards for secret surveillance that states must put in place to comply with the ECHR. Under Article 8(2) of the ECHR, interference with privacy rights can only be justified if it is in accordance with the law, pursues one or more legitimate aims and is

necessary for a democratic society to achieve those aims.

ECtHR embracing of mass surveillance regimes in Europe

States' safeguarding national security against acts of terrorism have long been accepted by the Court as a legitimate aim. In *Weber and Saravia v Germany* and *Liberty v United Kingdom* the ECtHR expressly recognised that national authorities enjoy a wide margin of appreciation in choosing how best to achieve national security, thereby acknowledging that bulk interception regimes do not *per se* fall outside this margin. In *Big Brother Watch*, the Court also confirmed that such measures are a lawful means for states to gather foreign intelligence, for early detection and investigation of cyberattacks, counter-espionage and counterterrorism. In doing so, the ECtHR endorsed the utility of bulk interception tools, considering these as "a valuable technological capacity to identify new threats in the digital domain". Yet, serious doubts have been raised on numerous occasions regarding the true effectiveness and therefore the necessity and proportionality of this practice. This is evidenced by a steady increase in global terrorist attacks since 9/11, whilst attesting to the unnecessary sacrifices of individual privacy and damage to foreign relations that they cause.

As a result of these judgements and the concomitant normalisation of mass surveillance, the ECtHR was criticised for fundamentally altering the existing balance in Europe

between the right to respect for private life and public security interests. Further, instead of outlawing bulk regimes altogether, the Court focused on establishing new procedural standards termed as "end-to-end safeguards", that must be present at every stage of operations (i.e. throughout the entirety of the intelligence cycle) and set out new criteria specifically for bulk surveillance schemes that domestic law must specify. It thereby signalled that states operating such surveillance regimes will be scrutinised henceforth against this benchmark.

New procedural safeguards for bulk interception of foreign communications

This approach may be viewed as problematic for at least two reasons. First, under Article 35 of the ECHR, the ECtHR will deal with the matter at hand only after all domestic remedies have been exhausted unless these are ineffective or their alleged ineffectiveness is the main contention made by the applicant. Since secret surveillance cases are decided *in abstacto* and given the Court's focus on procedural compliance of bulk surveillance regimes with the new safeguards established in the *Big Brother Watch* case, the ECtHR may be at the brink of pursuing a new trajectory and becoming the equivalent of a European Constitutional Court for privacy cases. Indeed, rather than scrutinising concrete violations of Convention rights and the need for a remedy by

the victim, the Court has agreed to review surveillance laws in general thus assuming the role of the court of the first instance at a national level and requiring the legislator to revise or amend the law in question when the Court considers it necessary. This, it has been suggested, marks a shift towards the ECtHR scrutinising the Convention states' legislative branches' respect for the rule of law and the basic requirements of law-making.

Secondly, the Court is prepared to hold violation of Article 8 rights far more willingly when it comes to states' domestic secret surveillance, compared to bulk intercepts of foreign communications, as attested by the *Zakharov* case and most recently in *Ekimdzhiev and Others v Bulgaria*. Here the ECtHR found that the Bulgarian law permitting secret surveillance, access and retention of communications of practically everyone in that country breached the right to privacy, as the law did not meet the "quality of the law" criteria. This is *inter alia* because parts of that law were insufficiently clear, the independence of the oversight body could not be guaranteed, whilst both the notification procedures and the remedies were ineffective. Consequently, the Court concluded that the Bulgarian law was incapable of keeping the surveillance to only that, which is necessary. The case sends a strong message to the CoE states: In a democracy secret surveillance powers must not be abused and governments must provide adequate, sufficient supervision and approval

to protect against abuse, together with the right to be informed. The question nevertheless remains as to how to reconcile the Court's apparent embracing of bulk interception of foreign communications so long as it adheres to the procedural guarantees, with its continued antagonism towards domestic secret surveillance methods.

The ECtHR's continued reliance on the security/privacy trade-off narrative

The ECtHR acceptance of bulk interception regimes as measures that in principle fall within states' discretion in fighting international terrorism seems to be predicated on the traditionally conceived privacy/security trade-off. Although the Court adopted a lenient approach to the issue of the "victim status" in surveillance cases, it has also shown to readily succumb to the security narrative. This is because it explicitly recognised the value of mass surveillance methods for security operations by supporting the CoE states' intelligence services pro-active approach in relation to unknown threats emanating from abroad. By doing so the Court is at the risk of discounting the complexities involved in the modern industry of mass surveillance, including the rationale for conducting it, the parties involved and the technical means at the disposal of state and non-state actors. Viewed through the prism of cost-benefit analysis, perhaps the cost of privacy and related human rights associated

with the upholding of this narrative far outstrips the security gains now and in the future.

Conclusion

Undoubtedly the post-9/11 anti-terrorism policy resulted in entrenching mass surveillance regimes particularly in Europe, with repeated scepticism as to its tangible benefits in terms of achieving national security. In this sense alone, the legacy of 9/11 will likely resonate for years to come and facilitate further expansion of state surveillance powers not only in consolidated but also in backsliding democracies. In Hungary and Poland, for example, the authorities have significantly expanded their surveillance powers without meaningful oversight mechanisms in place, whilst Polish security services have allegedly been using Pegasus malware to spy on the ruling party's opposition politicians. The ECtHR legitimising bulk interception practices coupled with the legislative branch often too willing to grant the executive blanket and unconditional powers of mass surveillance in the name of fighting international terrorism seems a flimsy bulwark against the surveillance industry. Yet, this is the unquestionable and unfortunate result of the global culture of counterterrorism narrative which has been successfully propelled by the politics of fear since 9/11.

Ralf Poscher und Michael Kilchling

Zwei Jahrzehnte nach 9/11 - Höchste Zeit für ein empirisch basiertes Monitoring staatlicher Überwachungsmaßnahmen

Eine der nachhaltigsten Veränderungen, die die Anschläge des 11. September 2001 in der westlichen Welt nach sich gezogen haben, ist die spürbare Beschleunigung der seit den späten 1980er Jahren zu beobachtenden Akzentverschiebung von einer reaktiven hin zu einer präventiv orientierten Sicherheitspolitik. Sinnbild dieser Entwicklung ist die kontinuierliche Ausweitung der Kompetenzen der Sicherheitsbehörden zur Überwachung verschiedenster Lebensbereiche der Bürgerinnen und Bürger. Diese langfristige „*Versicherheitsrechtlichung*" wird durch den rasanten technischen Fortschritt in der Digitalisierung wesentlich erleichtert – wenn nicht sogar befördert.

Sowohl die Verfügbarkeit potenziell sicherheits- und damit zugleich auch überwachungsrelevanter Daten als auch die Möglichkeiten für deren technisch unkomplizierten Transfer und ihre systematische/tiefe Auswertung durch staatliche Behörden (Sicherheitsbehörden ebenso wie Nachrichtendienste) haben sich signifikant verändert. Noch in den 1980er Jahren lag der Schwerpunkt staatlicher Überwachung zu einem wesentlichen Teil im Bereich der „klassischen" Telefonüberwachung; digital erfasste (Massen-) Daten etwa zur Mobilität, zu den Kommunikationsverläufen oder zum Surfverhalten im Internet, aus denen sich vielfältige Informationen mit potenzieller Sicherheitsrelevanz generieren lassen, waren entweder gar nicht verfügbar oder mussten einzelfallbezogen und personalaufwändig erhoben

werden, etwa durch längerfristig angelegte Observationsmaßnahmen.

Drei Beispiele intensivierter Überwachung seit 9/11

Vor allem in drei Bereichen wurde die Überwachung in Reaktion auf die islamistischen Terroranschläge systematisch ausgeweitet; dabei war jeweils die Europäische Union Impuls- beziehungsweise Taktgeberin. Der erste Anwendungsbereich betrifft den erweiterten Zugriff auf die Telekommunikations-Verkehrsdaten. Die bis heute gerade in dem konkreten Kontext der Verkehrsdatenüberwachung besonders kontrovers diskutierte Pflicht zur anlasslosen Vorratsdatenspeicherung wurde in Deutschland und einigen anderen Ländern überhaupt nur auf Druck der EU eingeführt. Die EU-Kommission wollte das Instrument damals bekanntlich um fast jeden Preis eingeführt wissen und hatte die Speicherpflicht mangels eigener Kompetenz zum Erlass sicherheitsrechtlicher Rechtsakte in der Prä-Lissabon-Ära ungeachtet der Kritik aus einigen Mitgliedsstaaten in eine wettbewerbsrechtliche Richtlinie gegossen (RL 2006/24/EG). Die beiden Begriffe Verkehrsdatenüberwachung und Vorratsdatenspeicherung werden in der öffentlichen Debatte seither mitunter fast wie Synonyme gebraucht. Auch die Rechtsprechung des BVerfG zur Vorratsdatenspeicherung und die daraus entwickelten ersten Ideen

einer Überwachungsgesamtrechnung (s.u.) beziehen sich im Wesentlichen auf diesen konkreten sachlichen Kontext.

Das zweite, ebenfalls europarechtlich determinierte Feld massenhafter Überwachung betrifft die präventive Geldwäschekontrolle. Dieses ursprünglich eng begrenzte, auf die (organisierte) Drogenkriminalität zugeschnittene Instrument wurde in Reaktion auf 9/11 auf die Bekämpfung der Terrorismusfinanzierung ausgedehnt. Die Idee der Verhinderung terroristischer Aktivitäten durch Überwachung der weltweiten Finanzströme wird seitdem zur Legitimation der kontinuierlichen und in immer kürzeren Zeitintervallen erfolgenden Erweiterungen (zuletzt 2021; eine weitere Geldwäsche-Richtlinie – es wird dann bereits die sechste sein – ist auf EU-Ebene bereits in Vorbereitung) angeführt. Sukzessive wurde daher auch in Deutschland ein umfangreiches Regularium zur flächendeckenden anlasslosen Speicherung von Finanztransaktionsdaten implementiert, die jeden und jede von uns nahezu unausweichlich trifft. Zusätzlich zu den Kundenstammdaten müssen jeder unbare Bezahlvorgang und jede Kontobewegung zusammen mit den dazugehörenden Begleitdaten (quasi eine Mischung aus „Verkehrs-“ und Inhaltsdaten) fünf Jahre lang gespeichert werden, nach einem Wechsel der Bankverbindung noch weitere fünf. In wenigen Lebensbereichen dürfte die Metapher des gläsernen Menschen der Wirklichkeit mittlerweile so nahe kommen wie hier.

Ein dritter, hier ebenfalls nur exemplarisch aufgezeigter Lebensbereich mit einer weitreichenden Überwachung auf Vorrat betrifft die Erfassung von Fluggastdaten auf der Basis der sog. PNR-Richtlinie der EU (RL (EU) 2016/681). Das zu ihrer Umsetzung eingeführte Fluggastdatengesetz (2017) verpflichtet die Airlines zur Übermittlung von bis zu 60 individuellen (20 größeren Merkmalsgruppen zuzuordnenden; vgl. § 2 FlugDaG) Informationen über sämtliche an deutschen Flughäfen abfliegenden und ankommenden Passagiere vor. Das betrifft neben den allgemeinen Flugdaten (Flugnummer, Flugziel, Abflug-/Ankunftszeit etc.) eine Vielzahl personenbezogener Informationen wie zum Beispiel Familienname, Geburtsname, Vornamen, Doktorgrad (*sic!*), Wohnadresse und Ausweisdaten des Fluggastes, sowie Vielfliegerstatus, Sitzplatznummer, Informationen zur Buchung und gegebenenfalls zu dem Buchungsportal beziehungsweise Reisebüro, Flugpreis und Kreditkartendaten, mitgeführtes Gepäck, mitreisende Personen und viele weitere. Anders als bei den TK-Verkehrs- und Finanztransaktionsdaten erfolgt die Speicherung nicht bei den privaten Dienstleistern, sondern unmittelbar beim Bundeskriminalamt (in seiner zusätzlichen Funktion als Fluggastdatenzentralstelle: Passenger Information Unit – PIU). Eine Reihe weiterer, originär nationalstaatlicher Kompetenzen wie die sogenannte Online-Durchsuchung ergänzen das aktuelle Anti-Terror-Instrumentarium.

Verfassungsrechtliche Diskussion zur Überwachungsgesamtrechnung

Die kritische fachliche Auseinandersetzung mit der hier nur bruchstückhaft skizzierten Entwicklung konzentriert sich im Wesentlichen auf die relevanten (verfassungs-) rechtlichen Aspekte. Dies gilt für Beiträge aus der systemisch-dogmatischen beziehungsweise legislativen Perspektive ebenso wie für Beiträge, die den Fokus eher auf die Anwendungsebene und die individuelle Betroffenenperspektive richten. Vergleichsweise wenig Aufmerksamkeit wird hingegen der Frage nach dem *tatsächlichen Umfang der Überwachung* zuteil. Auch in der Rechtsprechung des BVerfG spielt die Häufigkeit einer Maßnahme bislang allenfalls eine indirekte Rolle, wenn es etwa darum geht, durch die Aufstellung hoher rechtlicher Hürden die Anwendung besonders eingriffsintensiver Maßnahmen faktisch zu begrenzen. Unmittelbarer Bezugspunkt seiner Rechtsprechung ist bislang aber stets die Verhältnismäßigkeit der konkreten Maßnahme.

Spätestens mit dem Urteil zur Vorratsdatenspeicherung vom März 2010 (1 BvR 256/08) hat das Gericht auch eine andere Perspektive ins Spiel gebracht, indem es, über die konkrete Überwachungsmaßnahme hinaus, die Notwendigkeit einer Gesamtbetrachtung aller wesentlichen überwachungsrelevanten Kompetenzen der Sicherheitsbehörden ins Spiel

gebracht hat. Im Hinblick auf die freiheitliche Verfassungsidentität der Bundesrepublik, zu deren Kernbestandteilen das Gericht ausdrücklich das Verbot einer Totalerfassung und Registrierung der Freiheitswahrnehmung der Bürgerinnen und Bürger zählt, dürften die verschiedenen Kompetenzen in ihrer Summe nicht zu einer umfassenden Überwachung führen. Eine unzulässige (Total-)Überwachung sähe das Gericht bereits im Falle einer bloß theoretischen Rekonstruierbarkeit als erfüllt an. Daher müsse der Gesetzgeber bereits bei der Planung (das Gericht spricht wörtlich von „Erwägung“) neuer Speicherpflichten und Befugnisse zum behördlichen Zugriff auf bereits (irgendwo) gespeicherte personenbezogene Daten die Gesamtheit der verschiedenen bereits existierenden Datensammlungen und ihrer Nutzungsvoraussetzungen zu berücksichtigen. Dieses Prinzip ist generell zu beachten, auch jenseits des Bereichs der Vorratsdatenspeicherung.

Diese erweiterte Perspektive wurde in der Wissenschaft aufgegriffen und in ein Konzept zur ganzheitlichen Betrachtung des Überwachungsgeschehens übertragen, für das sich der auf Roßnagel zurückgehende Topos der *„Überwachungsgesamtrechnung“* (ÜGR) durchgesetzt hat. Mit dem etwas sperrigen Begriff wird auf die Notwendigkeit einer Gesamtbetrachtung des (jeweils aktuellen) Standes staatlicher Überwachung verwiesen, die alle einschlägigen präventiven und repressiven Überwachungs-maßnahmen

quasi aufaddiert. Der Koalitionsvertrag der neuen Bundesregierung greift den Ansatz der ÜGR wieder auf und betrachtet diese als ein wichtiges Element vorausschauender, evidenzbasierter und grundrechtsorientierter Sicherheits- und Kriminalpolitik.

Anders als der Begriff der Gesamtrechnung eigentlich impliziert, wurde die ÜGR in der Vergangenheit vor allem auf einer qualitativ dogmatischen Ebene diskutiert und nur in rudimentären Ansätzen operationalisiert. Beiträge aus der verfassungsrechtlichen Literatur halten sich meist im Vagen und begnügen sich weitgehend mit Vorschlägen, wie man die Gesamtheit der rechtlichen Befugnisse zur Überwachung abstrakt fassen und bewerten könnte. Völlig ausgeblendet wurde bislang die Frage, ob und gegebenenfalls wie häufig eine bestimmte Überwachungsmaßnahme und der damit verbundene Grundrechtseingriff zum Einsatz kommt; hier stochern wir bildlich gesprochen im Nebel. Wir können bislang nicht annähernd quantifizieren, in welchem Umfang sich die „Überwachungslast" in Deutschland seit 9/11 tatsächlich verändert hat, noch lässt sich deren Gesamtumfang bestimmen. Erst mit der Ausübung der verfügbaren rechtlichen Kompetenzen materialisiert sich der damit verbundene Grundrechtseingriff. Daher ist die *Kernfrage* nach dem – verfassungsrechtlich vertretbaren – Maß staatlicher Überwachung eben *auch eine quantitative*. Denn mit der Häufigkeit solcher Maßnahmen steigt auch die statistische Wahr-

scheinlichkeit und damit das Risiko der eigenen Betroffenheit. Der Blick auf zwei der eingangs genannten Beispiele macht es deutlich: während das individuelle Risiko, tatsächlich in den Fokus einer Online-Durchsuchung zu geraten, aufgrund der wenigen Einsatzfälle faktisch nahe Null liegt, betrifft die Fluggastüberwachung jeden und jede, die von einem deutschen Flughafen abfliegen und dort wieder ankommen (bzw. umgekehrt). Gleichwohl nimmt die Online-Durchsuchung in den wissenschaftlichen und (rechts-) politischen Diskussionsforen deutlich breiteren Raum ein als die Fluggastüberwachung.

„Überwachungsbarometer" - ein neues, empirisch unterlegtes Instrument zur Erfassung der realen Überwachungslast

Es erscheint mithin zwingend, das Überwachungsgeschehen nicht nur durch die dogmatische Brille zu betrachten, sondern parallel auch die empirische Realität in die Bewertung mit einzubeziehen. Dass das bislang nicht geschehen ist, kann jedenfalls partiell auch damit erklärt werden, dass belastbare statistische Informationen zur Häufigkeit der durchgeführten Überwachungsmaßnahmen insbesondere im präventiven Anwendungskontext lange Zeit gar nicht oder nur sporadisch verfügbar waren. Das ist eine entscheidende Lücke, die sukzessive geschlossen werden muss. Das Freiburger Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht arbeitet aktuell an dem

Konzept für ein periodisches Überwachungsbarometer, das die aufgezeigten Defizite aufgreift und damit ein empirisch unterlegtes Instrument zur Weiterentwicklung der ÜGR entwickelt. Ziel dieses neuartigen Modells ist es, die verschiedenen rechtlichen Überwachungskompetenzen und ihre normative Ausgestaltung (verfassungsrechtliche Perspektive) mit der realen Anwendungspraxis (empirische Perspektive) zu kombinieren. Auf dieser Basis kann das Überwachungsgeschehen gemessen und damit die Überwachungslast, der die Bürgerinnen und Bürger in Deutschland in einem bestimmten Referenzzeitraum (z.B. Kalenderjahr) ausgesetzt sind, sichtbar gemacht werden. Unterstützt wird das Vorhaben durch die absehbar zunehmende Verfügbarkeit aggregierter statistischer Daten.

Zur Erstellung eines realistischen Abbildes der Überwachungssituation und ihrer verfassungsrechtlichen Einordnung reicht es jedoch nicht aus, Zugriffsnormen und Anwendungszahlen rein quantitativ zu erfassen. Staatliche Überwachungsmaßnahmen und Zugriffe auf datenförmig hinterlegte Informationen müssen jeweils spezifiziert und im Hinblick auf ihre Zielsetzung und ihre Eingriffswirkung gewichtet werden. Beispielsweise dürfte ein nach abstrakter Bewertung eingriffsintensiver präventiver Echtzeit-Zugriff auf mobile Standortdaten einer in einem weitläufigen Waldgebiet vermissten Person oder ihrer Begleitperson zur Abwendung einer konkreten Gefahr für Leib oder Leben anders zu

bewerten sein als die repressive Abfrage von Kontodaten zur Aufklärung einer mutmaßlichen Geldwäsche-, Steuer- oder Vermögensstraftat. Beide könnten ihrerseits schwerer wiegen als etwa die massenhafte, potenziell Hunderttausende betreffende Verkehrsüberwachung mittels kennzeichenbasierter Abschnittskontrolle. Als entscheidende Parameter müssen daher sowohl die verfassungsrechtliche als auch die empirische Eingriffsintensität berücksichtigt und zueinander ins Verhältnis gesetzt werden.

Um die Eingriffsintensität der verschiedenen Überwachungsmaßnahmen bestimmen zu können, müssen diese nach einheitlichen verfassungsrechtlichen Kriterien typisiert und gewichtet werden. Hierfür wurde ein komplexes Kategoriensystem entwickelt, das alle abstrakt bestimmbaren Kriterien der Eingriffsintensität berücksichtigt und nach deren verfassungsrechtlicher Bedeutung jeweils unterschiedlich quantifiziert. Auch das BVerfG rekurriert in seiner Rechtsprechung sehr häufig auf die Schwere der Eingriffe und bewertet diese beispielsweise als nur „gering“ oder „geringfügig“ am einen, sowie „tiefgreifend“ oder „besonders stark“ am anderen Ende einer angedeuteten Skala. Eher in der Mitte einzuordnen sind wohl Maßnahmen von „erheblichem“ beziehungsweise „nicht unerheblichen Gewicht.“ Die genannten Beispiele sind weit entfernt von einer systematischen Kasuistik. Löffelmann spricht diesbezüglich in seiner Besprechung zum Bestandsdatenauskunft-

II-Beschluss nicht zu Unrecht von „Begriffssynkretismus“ (GSZ 2020, 182, 185). In der Tat wirken die zitierten Beschreibungen mitunter fast ein wenig hilflos. Was unterscheidet etwa einen *nicht un*erheblichen von einem erheblichen Eingriff? Auch die begrifflichen Unschärfen lassen erkennen, dass eine ausschließlich normative Bewertungsmethode zur Berechnung der Überwachungslast nicht geeignet ist. Bei dem Überwachungsbarometer geht es – anders als in der traditionellen Verhältnismäßigkeitsdogmatik – nicht um die abstrakte (verfassungs-)rechtliche Zulässigkeit oder Unzulässigkeit einer Maßnahme, sondern um ihre konkrete Eingriffswirkung bei den Adressaten. Aus dieser Perspektive ist *jede* Maßnahme ein Eingriff – auch die *verhältnismäßige*.

Um die Eingriffsintensität der verschiedenen Überwachungsmaßnahmen quantifizieren zu können, müssen die jeweiligen Umstände und potenziellen Folgewirkungen ihrer Durchführung in die Bewertung einfließen. Dies betrifft etwa die Voraussetzungen und Zielsetzung einer Maßnahme, die Durchführungsmodalitäten, Dauer und Streubreite, die Art der erhobenen Daten, ihre Verwendung einschließlich einer möglichen Weitergabe, ihre spätere Löschung, und viele weitere Umstände. Jedem dieser Parameter wird auf der Basis eines einheitlichen Kategoriensystems ein individueller Intensitätswert zugeordnet. Im Ergebnis kann die gleiche Maßnahme, zum Beispiel die Telekommunikationsüberwachung, in Bundesland A eine an-

dere Eingriffsintensität haben als in Bundesland B oder C. Dasselbe gilt, wenn solche Maßnahmen einerseits auf der Grundlage der StPO und andererseits im präventiven Kontext auf der Grundlage beispielsweise des BKAG oder eines Landespolizeigesetzes zur Anwendung kommen, wir auch das Bundesverfassungsgericht in seinem jüngsten Urteil zu den Überwachungsbefugnissen des Verfassungsschutzes (1 BvR 1619/17) noch einmal betont hat. Mit unserer aktuell getesteten Formel errechnet sich zum Beispiel für die präventive Abfrage von TK-Verkehrsdaten aufgrund der unterschiedlichen Ausgestaltung der aktuellen landesgesetzlichen Rechtsgrundlagen für fast jedes Bundesland ein anderer Intensitätswert; die Werte variieren auf der vorläufigen zehnstufigen Intensitätsskala um bis zu einen ganzen Punkt (das entspricht einer Varianz von 10 Prozent). Selbst im fiktiven Fall identischer Häufigkeit trügen die landesrechtlichen Maßnahmen in unterschiedlichem Maße zur Gesamtüberwa-chungslast in Deutschland bei.

Ausblick

Das neue Überwachungsbarometer versteht sich als ein rechts- und gesellschaftspolitisches Transparenzprojekt, das der interessierten Öffentlichkeit ebenso wie den verantwortlichen Akteuren in Wissenschaft, Politik und Justiz erstmals aussagekräftige, verständliche und leicht zugängliche

Informationen zu der realen Überwachungslast der Bürgerinnen und Bürger im täglichen Leben zur Verfügung stellt. Die methodischen Kernelemente wurden an anderer Stelle bereits ausführlich dargestellt. Im Zentrum der Projektarbeit steht aktuell die Feinjustierung der Formeln für die quantitativen und die qualitativen Parameter. Hierfür wurden zunächst zwei exemplarische Indexformeln entwickelt, mit denen die beiden Parameter rechnerisch unterschiedlich gewichtet werden; eine Formel ist nach oben offen konstruiert und orientiert sich stärker an der Häufigkeit, die andere ist stärker indexiert und fokussiert eher die Intensität der Zugriffe.

Die verschiedenen Berechnungsmöglichkeiten sind noch im experimentellen Stadium und sollen in den kommenden Monaten anhand erster Realdaten überprüft und auf ihre jeweiligen Effekte hin überprüft werden, wenn es etwa darum geht, wie quantitativ sehr wenige Maßnahmen mit sehr hoher Grundrechtsrelevanz wie die Online-Durchsuchung einerseits mit den massenhaften Zugriffen wie bei den Fluggastdaten andererseits, deren Eingriffsintensität nach unseren bisherigen Rechenmodellen relativ niedriger als die der Online-Durchsuchung anzusetzen ist, ins Verhältnis gesetzt werden können. Parallel hierzu werden auch verschiedene Darstellungsarten getestet, die das Überwachungsgeschehen erkennbar und die daraus resultierende(n) Überwachungslast(en) greifbar machen sollen. Neben der traditio-

nellen Darstellung in absoluten Zahlen kann die Zahl der jeweiligen Maßnahmen etwa in Form der durchschnittlichen Anzahl von Datenzugriffen pro Tag oder als Inzidenzwert bezogen auf 100.000 Einwohner angezeigt werden. So hat sich beispielweise die Gesamtzahl der behördlichen Kontoabfragen bei Kreditinstituten zwischen 2005 und 2018 von durchschnittlich 290 auf 3.758 Abfragen pro Tag beziehungsweise von 107,0 auf 1.353,3 Abfragen pro 100.000 Einwohner vervielfacht (siehe Projektbericht).

In der ersten Zeit wird das Barometer die Vielzahl an relevanten Überwachungstatbeständen zunächst nur selektiv abdecken können. Mit zunehmender Datendichte wird es immer besser in der Lage sein, Entwicklungen bereichs- und maßnahmenspezifisch zu identifizieren und Trends frühzeitig zu erkennen. Dabei können Änderungen des normativen Rahmens ebenso eine Rolle spielen wie Veränderungen der rechtstatsächlichen Rahmenbedingungen, etwa durch praxisrelevante gerichtliche Intervention und nicht zuletzt auch technologische Entwicklungen. Mit dem geplanten Modell dürfte es dann auch möglich sein, den faktischen Beitrag der verschiedenen Antiterrorismus-Befugnisse an der Überwachungsgesamtlast zielgenauer zu bestimmen.

Markus Naarttijärvi

Function Creep, Altered Affordances, and Safeguard Rollbacks

The Many Ways to Slip on a Slippery Slope

"According to this committee, it is thus hardly thinkable to provide possibilities for surveillance measures on such comparatively vague justifications as the terrorism act provides in order to provide protection against serious crimes in general. This would presume pervasive changes in the rules of criminal procedure that from a principled point of view would appear extremely dubious. There is in fact no doubt that the surveillance measures provided by the terrorism legislation deviate from the requirements of legal certainty that have traditionally been maintained in this country." – Committee on terrorism legislation, 1989 (SOU 1989:104 p. 219)[1]

"The fact that information can be obtained relatively broadly and unconditionally is necessary for the intelligence work to be conducted efficiently. Excessive regulation risks hindering collection in an undesirable way." – Swedish Government bill on law enforcement access to communications metadata (Prop. 2011/12:55 p. 84)

Leaving a paradigm behind

Stating that the terrorist attacks on 9/11 led to a paradigm shift in the political and legal approaches to surveillance of the private sphere is an observation so obvious it may sound like a platitude. Still, it remains valid. But where it used to be a statement about the events shaping our current paradigm, it may now soon become an observation of the past. We still don't know how the illegal, unjustified, and senseless war of aggression Vladimir Putin currently wages in Ukraine will impact the legal frameworks surrounding surveillance and privacy. But looking back at the 20 years of legal development since 9/11, is perhaps even more pertinent now, as it allows us to see not only that a shift occurred, but also more clearly how that shift was manifested. This in turn can teach us about what we may expect going forward.

In 2013, I published my PhD thesis on the rise of preventive electronic surveillance measures in Sweden. In it, I traced the development from the early days of telephone surveillance in the post-war era to the modern preventive electronic network surveillance and signals intelligence, focusing on the mandates provided to the Swedish Security Service (*Säkerhetspolisen*). Using constitutional proportionality theory as a lens, I sifted through preparatory works published between 1945 and 2013 to analyse the balancing

of security and privacy interests within the legislative processes leading up to expanding surveillance mandates.

Having gone through that process, I concluded my thesis on some rather gloomy observations. I found that legislators had largely failed to acknowledge the increasingly intrusive nature of surveillance that technological developments had brought. Statements on the privacy implications of certain measures were simply reused over the years with little consideration of fundamentally altered technological affordances shaping those implications.

As we know, the use of metadata surveillance to register numbers called from landlines in the 1960s is fundamentally different from the minute-to-minute geolocation and surveillance of mobile communication devices today. We also know that communications metadata can now be analysed on a larger scale, more quickly, and provide insights that even communications content may not. Yet, the same analysis of the privacy implications of metadata surveillance – holding it as significantly less sensitive than communications content surveillance – was essentially reused repeatedly and almost verbatim by legislators throughout the years.[2]

Another conclusion was that each reform towards preventive surveillance outside of the context of criminal procedure was presented as non-exceptional, once that first step had been taken. Each successive step from the paradigm

of reasonable suspicion towards an increased role of risk-based logic would look back on a previous example that proved that this new proposal was neither unprecedented nor exceptional. Looking a bit closer at those legislative precedents, however, reveals even more clearly the fundamental shift that happened during the years following 9/11.

A temporary firewall

The first real, albeit limited step towards preventive surveillance mandates in Sweden was taken in the early 1970's through the "Terrorist Act".[3] This Act provided a narrow set of measures for when the deportation of a person believed to be a member of a terrorist organisation could not be carried out on account of non-refoulment concerns.[4] The targeted individuals (usually numbering no more than 0-3 persons in a given year) could then be made subject to certain preventive surveillance measures, including the tapping of phones following a court order. The measures were intended to ensure that these individuals or an organisation they belonged to or acted for did not engage in terrorist activities while remaining in Sweden. In establishing this measure, the legislator made it clear that it constituted a significant departure from established privacy norms and legal safeguards, and that the legislation could be accepted only as it pertained to a very limited cadre of individuals, already subject to eventual deportation on national security grounds.

For some time, this firewall of principle separating the wider public from similar measures held fast. In the wake of the murder of prime minister Olof Palme in 1986, a parliamentary committee considered widening the Terrorist Act to Swedish citizens and foreigners not yet subject to deportation orders, but ultimately found that "the evidentiary requirements in the regulations are so low that it can hardly be considered justifiable to provide for the possibility of coercive measures in the event of even weaker suspicions." (SOU 1988:18, p. 170-171). They also concluded that the exception for foreigners subject to deportation orders could "be considered justifiable only as an outgrowth of our right to decide for ourselves which foreigners are allowed to stay in this country. To make further exceptions is out of the question." (Ibid. p. 175). The following year another inquiry tasked with evaluating the need for wider preventive surveillance measures found that such a proposal would unacceptably undermine established rule of law principles. These findings were reached despite the committees being mindful of "the ever-increasing or at least uninterrupted high frequency of terrorist acts and their geographical spread" (SOU 1989:104, p. 179).

The new reality

With the terrorist attacks on 9/11 and in London and Madrid in the following years, this firewall began to crumble. In ac-

cordance with the trend in most western states, what was once regarded as unacceptable from a rule of law standpoint slowly became implemented as part of the new security paradigm. Through the "2007 Prevention Act"[5] the Swedish Security Service was given a wider mandate to use preventive electronic surveillance to counter-terrorism and certain other crimes against national security. In justifying this measure, the government leaned against the existing rules in the Act on measures against foreigners subject to deportation, arguing that the new measures were not, in fact, unprecedented or a significant departure from existing norms. A line of argument that required some very skilful cherry-picking from the historical context and previous legislative deliberations. In fact, the new rules must be seen as a legal watershed moment towards a normalisation of the preventive security paradigm and caused a fundamental shift in how covert surveillance could and would be deployed.

The next significant step was taken in 2012 when measures for preventive metadata surveillance was introduced. The new law, colloquially called "the Gathering Act",[6] gave law enforcement agencies access to historical (as opposed to real-time) communications metadata, including the past location of specific communication devices. This Act is significant in two regards. First, the government – as apparent from the quote at the beginning of this essay – specifi-

cally intended a broader and more unconditional gathering of communications data. This led to the adoption of conditions for access to information based not on specific levels of suspicion, but rather the benefit of the information could bring for law enforcement agencies, i.e., whether it could be of "particular importance" in preventing, deterring, or detecting crimes that could warrant a prison sentence of two years or more. Second, the legislator did not find it suitable to place the authorisation for these surveillance warrants on any external authority like a court, but rather internally within law enforcement agencies themselves. The rationale for this was based mainly on practical and organisational concerns relating to expedience, but the government added the more principled argument that unlike in the criminal investigation context, the privacy dimension in intelligence operations was not characterised by an adversarial dimension but rather displayed more of a "citizen perspective", which was not as well suited for courts to decide on (Government bill. 2011/12:55, p. 88-89).

There is so much one could say on that point, but I'll settle on observing that perhaps the government felt that law enforcement agencies with a vested interest in access to data would, in fact, be better suited to take that citizen perspective into account than a court of law. More likely however is that a court might get in the way of that "more unconditional" gathering of communications data the gov-

ernment had in mind. In 2019, the power to authorise the gathering of meta-data was moved to prosecutors who are organisationally separate from the police authorities. This was a result of the Tele2 judgment (Joined Cases C-203/15 and C-698/15), requiring authorisation by a court or independent authority. It is uncertain if this move fulfils the requirement of an independent authority, but it must be seen as a step in the right direction.

These reforms may well be described as examples of surveillance or function creep, in that they represent a stepwise and creeping expansion of surveillance mandates. Further expansions of preventive surveillance measures to counter organised crime are currently being considered, so the development has by no means stopped.

Safeguard rollbacks

It is however also worth highlighting a parallel development of equal importance, through what could be described as *safeguard rollbacks*. These are different from surveillance creep, in that the aim and purpose of surveillance mandates remains largely the same, but the associated safeguards are gradually weakened. These rollbacks have generally taken place where mandates were initially put in place with strict limits to ensure proportionality and legal certainty, but where the effectiveness of those mandates is later argued to be limited due to the safeguards themselves.

A telling example is how the government changed the legal definition of which individuals could be subject to preventive surveillance by the Swedish Security Service in the previously mentioned 2007 Preventive Act. When the act was initially proposed, the legislator took care to differentiate it from the rules established in the 1970's Terrorist Act. A more significant individualised assessment was highlighted as a safeguard, where the association with a specific organisation would not be a determining factor, only whether there were "particular reasons to assume" that a specific individual would commit a specific range of serious crimes, such as terrorist crimes. This essentially created an evidentiary standard for interferences where credible information was needed to point towards future specified crimes.

A subsequent evaluation found, however, that this requirement became difficult to reach in practice. Actual evidence of future possibilities was both difficult to come by and would end up leading to the opening of a formal investigation into preparatory offences. This analysis eventually led to a revised threshold implemented in 2015. This was based on whether there was a 'significant risk that a specific person would engage in' certain serious criminal activities. The organisational connection now made a comeback, as this 'significant risk' threshold in relation to a the specific individual would be lowered in cases where there was a significant risk that an organisation the individual "belonged

to or acted in support of" would engage in serious criminal activities. In such cases, the threshold would be reduced in relation to the individual, where it would suffice that the individual "may be likely (*befaras*)" to support these activities.

Another example can be found in the legal rules surrounding the collection of signals intelligence in electronic communication networks. When in 2008 the Swedish defence radio establishment (FRA) was given the mandate to collect signals intelligence in fibre optic cables carrying electronic communication to and from Sweden, the fierce public and political backlash surrounding the reform forced the government to draw clear boundaries between law enforcement and military intelligence gathering. It was said that the signals intelligence conducted to further defence interests were aimed at foreign threats to national security and would not be allowed to undermine the rules governing the use of electronic surveillance under the rules of criminal procedure. As such, both the Swedish security service and the national police were initially excluded from directing the intelligence gathering but could still receive intelligence reports relevant to their tasks from the defence radio establishment.

In 2013 however, the Swedish Security Service and the National Operations Department of the police were given the mandate to direct signals intelligence gathering towards phenomena they had an interest in. To compensate for this

new mandate, police agencies were not allowed to receive intelligence about matters relating to ongoing criminal investigations. Eventually, the government found that this was impractical. It could lead to a situation where if information emerged that indicates that an international terrorist organisation was planning a terrorist attack in Sweden, and the suspicions would reach such a level a preliminary investigation was opened, the FRA would need to suspend its reporting to the authority. Hence, in 2019, this limit was also removed. Instead, a rule was issued stating that the national police and the security service could not use the information they received within criminal investigations and information from signals intelligence should (as a main rule) not be given to persons involved in such investigations.

What have we learned?

In light of the Swedish example, we can see developments in government electronic surveillance occurs along at least three developmental axes. First, there is the increased depth of surveillance measures in terms of the resolution of the picture that they draw of the individual, driven to a significant degree by changes in the underlying technologies of communication and data processing. On the second axis is the expansion in terms of width or scope, i.e., the range of individuals, groups, or phenomena potentially subject to surveillance. This is where most discussions of surveillance

or function creep will tend to focus, and we can indeed see that the concept is alive and well in Sweden in relation to preventive surveillance. Finally, on the third axis, we find the safeguards implemented to prevent abuse of the measures implemented along the first and second axis. Here, the Swedish example suggests that we need to pay closer attention to safeguard rollbacks. The sometimes intricate and legal-technical nature of these rollbacks is less likely to attract political and public interest, yet they may carry far-reaching implications in the practical effects of surveillance mandates. Proportionality reviews by European Courts have so far proven to be the main limit to government ambitions in this regard, as they tend to place great emphasis on existing safeguards rather than placing outright limits on surveillance as such. Finally, along all these axes we need to pay close attention to changes in the technological affordances which may alter the practical effects of legal mandates or allow the introduction of methods to arise within or in between existing mandates. As the mandates and legal safeguards surrounding surveillance begins to face the capabilities provided by technologies of machine learning and automated decision-making, this is likely to become more important than ever.

References

1. All translations are the author's own.
2. This continued until the CJEU acknowledged the implications of metadata surveillance in the *Digital Rights Ireland* and *Tele2* judgements, essentially equating the privacy implications to that of content surveillance and thereby forcing the legislator to change approach.
3. The official name was Lag (1973:162) om särskilda åtgärder till förebyggande av vissa våldsdåd med internationell bakgrund ('Act (1973:162) on special measures to prevent certain violent acts with an international background').
4. The organisation the individual was engaged in would also, through their previous activities, have to have shown that they systematically used foreign land as a scene for violent actions with political purposes.
5. The official name is Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ('Act 2007:979 on measures to prevent certain particularly serious crimes').
6. The official name is Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ("Act (2012:278) on the gathering of information about electronic communication in law enforcement authorities intelligence operations").

Pika Šarf

Something Wicked This Way Comes

The Tale of Indiscriminate Surveillance, the State of Permanent Crises and the Demise of the Data Protection Afforded to Third Country Nationals

Writing in the aftermath of 9/11 terrorist attacks, Steven R. Salbu noted:

> *"Since EU and U.S. political interests are largely aligned in the war against terrorism, it is possible that the EU will move closer to the U.S. as a result of the attacks, rather than the U.S. moving away from the EU. To the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programs."*

One crisis after another was offered as a justification for the establishment of a comprehensive surveillance apparatus, while TCNs were gradually stripped of their rights to privacy and data protection, transforming the movement of innocent individuals into suspicious, potentially terrorist activities. Among the most significant changes in information management in the area of freedom, security and justice (AFSJ), interoperability – the ability of information systems to exchange data – will have the most profound effects on the right to data protection and as such marks the "point of no return". This contribution will seek to answer the question, how did we get to this point, and more importantly, where do we go from here?

Knowledge is power

On 6 June 2013, Snowden's revelations exposed a mass surveillance programme conducted by the U.S. National Security Agency, which for decades had been secretly gathering intelligence on the entire foreign population, including their political leaders, international organisations, and businesses. While the United States vigorously defended the legality of its intelligence gathering programmes, predominantly by leaning on the argument of their indispensability in the fight against terrorism, the international community was unanimous in condemning bulk and systematic blanket collection of (personal) data. The European Parliament was among the most vocal critics of both the surveillance practices as well as the flawed rationale behind them. In its Resolution, adopted on 12 March 2014, it stated that

> *"the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; [...] such programmes are incompatible with the principles of necessity and proportionality in a democratic society."*

What is more intriguing to look at is what the European Parliament stayed silent on, in particular, what it failed to say about the EU's data-gathering practices in the fight against terrorism and serious crime. At that time, all of

the EU information systems in the AFSJ that are in use today, namely the second-generation Schengen Information System (SIS II), the Visa Information System (VIS) and the European Asylum Dactyloscopy Database (Eurodac), were already fully operational. Two of them (SIS II and Eurodac) had just undergone a major transformation from purpose-specific centralised databases with narrowly defined access rights to more general, security-oriented investigative tools. Additionally, the EU had been contemplating the idea of establishing two additional databases, the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS), and making all of the AFSJ information systems interconnected in order to enhance the level of security while facilitating travel for *bona fide* TCNs. None of the initially proposed measures was adopted at the time. However, that does not mean that they were off the EU's agenda, but rather that they were hibernating, waiting for the right moment to be brought back to the table.

Crises in the EU as the catalyst of enhanced surveillance

The terrorist attacks that occurred in Paris in January and November 2015, and at the beginning of 2016 in Brussels, coupled with the peak of the migrant crisis, fuelled the security agenda of the Juncker Commission. The EU institutions stood united in condemning the tragic events that shocked

the old continent and immediately announced new counter-terrorism measures to be adopted. Following the trend of blurring the lines between immigration management, border control, law enforcement and broader (internal and external) security prevention, strengthening control of the external borders of the Union became one of the top priorities in the EU's fight against terrorism, and "*stronger and smarter information systems*" were at its core. While in the European Agenda on Security, which was adopted at the beginning of 2015, a shift towards more generalised surveillance of third-country nationals was already perceptible the Agenda does not urge for the introduction of new measures but rather calls for the reform of the existing tools and their use to the fullest extent possible. However, the documents adopted in 2016 show a noticeably different picture – a picture of Europe striving to "*regain control over the external borders*" by pushing for numerous previously withdrawn legislative proposals and introducing a plethora of new ones with the aim of ensuring a high level of internal security. In the following three years, the legal basis for the establishment of three additional centralised databases was adopted (EES, ETIAS, ECRIS-TCN), information exchange was intensified by the revision of two of the existing information systems (SIS II and VIS), while the proposal to reform Eurodac is still being negotiated as a part of a wider transformation of migration and asylum policy in the EU.

EU in crises meets technical feasibility: Interoperability of information systems in the AFSJ

Finally, in May 2019, all of the previously separated AFSJ databases became interoperable – or at least are on the path towards becoming interconnected once the proposed measures become operational – with the adoption of two Interoperability Regulations (Regulation 2019/817, Regulation 2019/818). Interoperability as "*the ability of information systems to exchange data and to enable the sharing of information*" will consist of four components: the European Search Portal, the Shared Biometric Matching Service, the Multiple Identity Repository and the Multiple Identity Detector (detailed description of the components is available here). They will enable separate information systems to start *talking to each other* in order to fill the blind spots created by the compartmentalised approach to AFSJ information systems. EU documents and proposals continuously endorse the position that reduces the concept to a purely technical matter, explicitly stripping it of any political or legal connotation by stating that "*interoperability is a technical rather than legal or political concept*". By endorsing the position of interoperability being a technical choice, the debate surrounding the adoption of the Interoperability Regulations mainly revolved around the question of whether the proposed measures were technically feasible, rather than compatible with the human rights regime in the EU, especially with the right

to data protection. This position was met with fierce opposition from the institutions entrusted with the protection of human rights (e.g. EDPS, WP29, FRA). They recalled with a single voice that interoperability will profoundly change the information sharing apparatus in the EU, thus the choice to implement it should be made upon thorough consideration of all relevant factors, not merely technical feasibility. Confusing legal with technical repercussions precludes having a proper debate from the human rights perspective. Yet, by reducing interoperability to a purely technical concept and then allowing the technical feasibility to dictate political choices without clearly specified aims of the measure, the risk is that interoperability becomes an end in itself.

Where to next?

When assessing surveillance measures at this critical moment in time, when the world is faced with the Covid-19 pandemic, it is perhaps more than ever important to look into the past to better understand what may lie ahead for us. Once again, we are faced with an unprecedented threat, similar to the situation in 2001, when the 9/11 terrorist attacks forever changed the intelligence-gathering practices of the global community. With the global spread of Covid-19, a highly contagious disease with a large percentage of asymptomatic cases, the adversary today is more intangible than ever. As a consequence, countries may feel the urge to

extend the scope of their surveillance practices a step further, by subjecting their citizens to constant monitoring.

The idea is nothing new; quite the contrary. Already during the discussions regarding the Smart Borders Package there arose an idea to monitor the border crossings of all travellers, not just TCNs, either in the Entry/Exit System or in a separate large-scale database. If (or better, when) border controls are no longer a measure of immigration control and internal security, but rather a measure to contain the spread of the deadly virus, which does not differentiate between EU citizens and third-country nationals, it becomes much easier to justify the surveillance of the entire population. In fact, this would not be the first privacy-invading measure imposed in the fight against Covid-19. Numerous countries introduced contact-tracing applications, while others were even subjecting infected individuals to mandatory geolocation tracking enabled by wearable technology. Although the majority of the solutions being developed in the EU attempt to preserve privacy and are in line with the established data protection regime, it is undeniable that they have the potential to reveal certain aspects of our private lives. The arguments put forward by governments worldwide in favour of the new wave of highly sophisticated digital surveillance tools are strikingly similar to the post-9/11 rhetoric: every one of us will have to give up a bit of our privacy to survive as a community.

Marcin Rojszczak

Electronic Surveillance in a Time of Democratic Crisis

Evidence from Poland

Against the background of the continuing democratic crisis in Poland, attention is increasingly being paid to the progressive expansion of state surveillance powers. While these trends began around the same post-9/11 shift towards securitizations that many states experienced, in Poland, expansive surveillance also correlates with the populist shift that started in the mid-2010s.[1] The correlation between non-democratic forms of government and extensive surveillance powers is not a new phenomenon. It characterises both authoritarian states and those *quasi-democracies* drifting towards them. As before in Hungary, the ruling majority in Poland is not only trying to monopolise all public institutions, including the judiciary but also systematically attempting to extend the scope of surveillance powers. These changes are accompanied by a weakening (or complete removal) of the legal safeguards that normally serve to counteract the risk of abuse of power in a democracy. The Polish example is also interesting because it allows one to assess the relationship between the evolution of surveillance powers and the formation of non-democratic forms of government. In particular, it begs the question; is it undemocratic governance that leads to the creation of elaborate forms of surveillance, or is it the other way around? And further, is it overly broad surveillance powers that inevitably lead to the erosion of democratic principles, ultimately corrupting those in power?

Expansion of surveillance powers

In Poland, the problem of using extensive surveillance powers is discussed mainly in the context of criminal procedure. As a result, unlike, for example, in Sweden or Germany, Polish regulation on the use of electronic surveillance in the intelligence field (foreign or domestic) is not publicly debated at all. This is because national regulation in this area is very broad and of a blanket nature. However, to summarise these regulations simply as ‚incomplete or requiring improvement' would be an oversimplification. The Polish legislature has not defined any limitations nor established any legal safeguards for the Intelligence Agency (*Agencja Wywiadu*) regarding its foreign electronic surveillance activity. At the same time, credible reports exist of serious abuses by Polish security services involving the bulk collection of electronic communications and the transfer of several million items of intercepted data to the US National Security, beginning around 2009 and revealed by Edward Snowden's leaks.

By contrast, electronic surveillance measures used in the fight against crime have been an enduring element of public debate. The need to increase the effectiveness of law enforcement agencies has been the main argument used by the ruling majority in recent years to maintain existing and establish new surveillance measures.

For these reasons, neither the government nor the constitutional court have ever challenged the legitimacy of a general data retention obligation – even in the context of collecting data for criminal investigations. As a result, domestic retention laws have not changed for more than 10 years and are still a direct transposition of the EU Data Retention Directive, annulled by the CJEU back in 2014. Moreover, in Poland, access to retention data is not preceded by any form of judicial review, which *per se* is not compatible with the Charter of Fundamental Rights.

At the same time, retained data is an important source of information for law enforcement agencies. According to the Ministry of Justice, the police and security services gather 1,5 million pieces of data from telecommunications systems every year. This number is increasing year on year, with no discernible decrease in crime or other objective reasons to justify this practice.

Poland is also a country where a number of new mechanisms for collecting data on citizens have been introduced in recent years. One example is STIR – an IT system that is (or should be) used by the tax authorities to collect data from financial institutions on their clients, including accounts held and transactions made. STIR contains billions of records that allow one to trace the financial transactions of a large part of society. It is impossible to see how small everyday transactions are supposed to help combat serious

tax crimes, such as VAT carousels. Nor have the authorities demonstrated the need to automatically collect and process – as they do – data on a large number of taxpayers, including those for whom there is not even an even indirect link to tax offences. This process is beyond the control of the courts. Moreover, while formal approval by the prosecutor or the court is still required for the security services in order to obtain data directly from financial institutions, accessing the same information using the STIR database can be carried out without any authorisation or external control whatsoever. This excessive amount of data on citizens and unchecked access to it clearly raises questions about the proportionality and legitimacy of the measures taken to gain it. Similar doubts have been raised about targeted surveillance measures.

Since the current Polish government came to power in 2015, there have been a number of regulatory changes that have reduced the effectiveness of pre-existing legal protections.[2]) One example is the removal of a provision prohibiting the use of illegally obtained evidence in criminal proceedings. The new government-dominated legislature not only sanctioned the use of this type of defective evidence but also established a norm whereby excluding evidence on the grounds that it was obtained in violation of the law effectively became prohibited. In this way, a kind of *anti-safeguard* was introduced in the Polish criminal procedure –

creating an incentive to conduct extrajudicial surveillance. It is difficult, if not impossible, to explain the need for such an extraordinary mechanism in a democratic state.

Deformation of independent control

The impact of these expanded surveillance powers on individual rights and freedoms could be partially reduced if effective control mechanisms were introduced. In fact, the essence of the abuse of power is not the acquisition of information by public authorities, but the ability to use it in carrying out their own – possibly illegal – activities. Taking this into account, the purpose of exercising control over state surveillance activity is not only to prevent individual cases of surveillance where it is not required but to also prevent the occurrence of systemic violations where the authorities remain beyond any real legislative control and are free to pursue their own agendas.

In Poland, no dedicated bodies to supervise state surveillance activity have ever been established. Therefore, the entire burden of control in this area is exercised by the courts of law. Prior review is used in surveillance cases pertaining to criminal procedures. As mentioned earlier, in Poland, this type of control is not only applied in the case of obtaining metadata but also in some cases of the surveillance of foreigners. Formally, the court authorising

the surveillance should verify that the condition of necessity has been met and confirm that the requested measure is the least invasive among those available. In practice, however, a prior review has not been used properly for many years now – as evidenced by the fact that courts accept more than 95 % of requests for surveillance (see e.g. data from 2018, 2019 and 2020). In some cases – for example, applications made by the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*) in 2017 – all (100 %) of the applications submitted to the court were approved. This means that, in practice, there was not one single case where the court had any doubt about the need for the surveillance measures requested. This is a remarkable statistic and one which strongly suggests that this control mechanism lacks effectiveness. Such a conclusion is supported by the case law of the ECtHR, which, when examining a similar case, concluded that the unusually high rate of accepted applications indicated that „investigating judges do not address themselves to the existence of compelling justification for authorising measures of secret surveillance."

Blanket approval of surveillance requests is not the only deficiency in judicial review in Poland. Similarly ineffective is the biannual verification of law enforcement agency reports on the scope of metadata collected from telecommunications systems. This verification is carried out without clearly defined standards, is random in nature, and in many

cases, the court itself has concluded that on the basis of the data presented, it has proved impossible to determine whether law enforcement agencies have acted within the scope of the powers granted to them. Yet this mechanism continues to remain in place without any kind of legislative initiative taken to address its glaring weaknesses.

Surveillance state in action? The 2022 Pegasus case

Overly expansive surveillance powers combined with the erosion of their oversight inevitably lead to abuse of power. In 2018, it was reported in the media that one of Poland's security services, the Central Anti-Corruption Bureau (CBA), had purchased Pegasus – a modern electronic surveillance software programme – from the Israeli NSO Group. It is worth recalling that the CBA is a service that was created by the current government the last time it was in power, back in 2006, and that the Bureau has a reputation not for fighting against corruption, but for conducting illegal activities motivated by political reasons. It is not surprising, therefore, that the purchase of Pegasus by the CBA generated discussion not about increasing the effectiveness of the fight against crime, but about the risk of the tool being used to pursue political ends.

These suspicions were confirmed in early 2022 when Citizen Lab and Amnesty International provided evidence of

Pegasus being used to eavesdrop on a key opposition politician, and on a lawyer acting in disputes with the government and public prosecutor about abuses of power. As a result, public attention was once again drawn to the problem of excessive surveillance powers and the lack of control over their exercise.

The outbreak of war in Ukraine has caused other issues – including those related to the surveillance affair – to be pushed into the background for the time being. It is worth noting, however, that the Pegasus affair has not led to any in-depth reflection on the need to reform the entire Polish surveillance framework. What is more, the current government not only, it seems, fail to see any need for change, but conversely, maintains that the current regulatory model is wholly adequate, obviating the need to either create new or strengthen existing mechanisms of control over the activities of special services.

Final thoughts

There is no doubt that authorities must have effective tools to both protect national security and conduct the fight against crime. At the same time, the understandable secrecy surrounding the work of the security services must not create an opportunity for the abuse of power. Surveillance

without adequate control weakens democracy, leads to a distortion of its principles, and ultimately, as the ECtHR has warned, threatens its very existence.

The current model of Polish surveillance regulation is the result of many years of neglect and the mistaken conviction of those in power that a state is limited in its freedom to make decisions becomes weak. However, being effective is not the only (and for many, not the most important) goal of the government. Suffice it to say that though authoritarian states are usually *effective* in achieving the goals of those in power, this does not mean that their form of government can be considered superior.

The Polish experience demonstrates how a determined populist government, using the tools available in a democracy, can in a relatively short space of time erode legal safeguards established to control state surveillance activity. This is a scenario that has already played out in Poland, and there is no reason to assume that it cannot be repeated in other countries, including those with – for the time being, at least – well-established democratic governments.

References

1. Applebaum Anne, Twilight of Democracy: The Failure of Politics and the Parting of Friends (London: Allen Lane, 2020).
2. Sadurski Wojciech, Poland's Constitutional Breakdown (Oxford University Press, 2019).

Stuart Hargreaves

Hong Kong Surveillance Law

From 9/11 to the NSL

In this short piece I suggest that though 9/11 did not immediately result in a dramatic expansion of the surveillance state in Hong Kong as was often seen in the west, twenty years later a similar process is now well underway. Though Hong Kong's surveillance and privacy laws have long been relatively deferential to the needs of law enforcement, the dramatic legal changes occasioned by the introduction of a new "national security law" in 2020 suggest that the population will be under increasing forms of surveillance in the coming years.

The legal aftermath of 9/11

Perceived to be at relatively low risk of a terror attack itself, the initial legislative responses to 9/11 in Hong Kong were not directly concerned with public surveillance specifically, or even domestic security generally. As an international financial centre, it was clearly of importance for Hong Kong to implement Security Council Resolutions 1373 and 1390 in the immediate aftermath of 9/11. The first of these required States to prevent and suppress the financing of terrorist acts, while the second expanded pre-existing sanctions against Al-Qaida, the Taliban, and associated entities. Hong Kong had to wait for instructions from Beijing before proceeding, as both Resolutions clearly touched upon matters of state and foreign affairs – exclusively the domain of the Central People's Government (CPG) under Art. 13 of

the Basic Law, Hong Kong's quasi-constitution. Even after approval from the CPG the process of drafting and implementing the UN (Anti-Terrorism Measures) Ordinance was uneven. Nonetheless, shortly after its introduction the Government quickly moved from this largely finance-focused legislation to the broader "national security" area.

Art. 23 of the Basic Law obliges Hong Kong to introduce laws that prohibit various acts that threaten the state, such as treason, secession, subversion, and so on. In 2002, the Security Bureau published its plan to introduce such legislation, and in early 2003 the National Security (Legislative Provisions) Bill was introduced to the Legislative Council. In addition to creating a series of new criminal offences, broad powers were given to the police to execute warrantless searches to preserve evidence related to the new crimes. Fears were raised that many of the proposals might threaten civil liberties (a useful primer on the key concerns can be found here). After widespread street protests against the Bill, the Government eventually withdrew it and offered no timeline for re-introduction. This meant that the laws of Hong Kong, as related to surveillance and privacy, were not significantly restructured in the years that immediately followed 9/11.

Surveillance & intercept laws

In part, this was because even without the introduction of new laws under Art. 23 of the Basic Law, legislation already on the books in the early 2000s gave quite a free hand to the Government to conduct surveillance. The Telecommunications Ordinance was enacted by the colonial government in 1962 (the link shows the law as it stood in 2003), and allowed the Governor to order the interception of any message transmitted by a telecommunications system if he believed it to be in the "public interest". The Secretary for Security declared that the "public interest" in this context meant the "prevention or disruption of serious crime, or necessary in the interests of the security of Hong Kong". This scheme was based on a provision of the UK Post Office Act that had been found by the European Court of Human Rights to be inconsistent with the right to respect for one's private life and correspondence in 1984. Local concerns were voiced about the broad authority the Telecommunications Ordinance gave to the Governor, particularly after the introduction of the Bill of Rights Ordinance in 1991. Though a 1996 Law Reform Commission report recommended a significant update to the law, no changes were made. With the transfer of sovereignty over Hong Kong on 1 July 1997, the Chief Executive replaced the Governor as the party with the power to order communications intercepts.

However, the coming into force of the Basic Law on that same date also resulted in the development of an expanded power of constitutional review. In 2006, the scheme created by the Telecommunications Ordinance was declared an unconstitutional restriction on the freedom of communication and privacy rights contained in the Basic Law. The Court concluded that the virtually untrammelled power given to the Chief Executive was incompatible with the principle that any restriction on those rights had to be proportional and done "in accordance with legal procedures". The Court gave the Government six months to come up with a framework; the result was the introduction of the Interception of Communications & Surveillance Ordinance (ICSO).

The ICSO

The ICSO created a system of authorisation for both the interception of communications and the placing of individuals under covert surveillance that was out of the hands of the Chief Executive. Interception is defined in the law as inspecting the contents of a communication during transmission. There are two forms of covert surveillance contemplated – that engaged in circumstances under which the target would reasonably expect to be seen/heard, and those in which they would not. Interception and the latter form of surveillance both require *judicial* authorisation, while the former can be authorised by an officer of sufficient rank.

The ICSO also creates a system of external oversight in the form of mandatory annual reporting and the presence of a quasi-independent Commissioner on Interception of Communications & Surveillance. But while from the perspective of the privacy interests of Hong Kong residents this was clearly an improvement over the Telecommunications Ordinance, the ICSO is still relatively deferential to the needs of law enforcement.

Most obviously, the narrow definition of what counts as an "interception" means that no authorisation at all is required for the police to collect metadata about communications; metadata, of course, can reveal a tremendous amount of detail about a person. The requirement for authorisation also only occurs 'in the course of transmission', meaning that once a digital message is delivered, attempts to access it falls outside the ambit of the law. In the era of "the cloud", this has important consequences. The licence required to operate an ISP or mobile phone service in Hong Kong allows them to disclose information about their users for the prevention or detection of a crime. The former Secretary of Security evaded questions about whether this means the police do not need to follow the ICSO requirements in the context of emails or text messages.

The most recent transparency report (2018) showed that between 2011 and 2017, Government departments made an average of about 4500 requests per year to telecommunica-

tion and internet companies for user information. 88 % of those requests were made by the police, which stated they did not track how many of those were accompanied by a warrant. While not strictly contemplated by the law, until 2019 the police appear (1, 2) to have been able to not only access user information but also obtain the removal of certain content online by leveraging a combination of the aforementioned procedure and accusations that users were believed to have committed the offence of "accessing a computer with dishonest intent". This was particularly apparent during the street protests of 2014, known as "Occupy Central".

The ICSO also does not speak to "public" forms of surveillance such as the use of CCTV cameras, or the broad gathering of information, generally in a non-targeted manner. Hong Kong's data protection law – the Personal Data (Privacy) Ordinance (PDPO) – does deal with information flows, but not in a manner that might meaningfully restrict modern forms of "dataveillance" by law enforcement. Enacted in 1995 (and amended since then only to deal with direct marketing), the PDPO is a relatively conventional data protection regime that implements a version of the "fair information principles". The law defines "personal data" as any data relating to a living individual from which that individual may be identified, and that exists in a form that makes processing reasonably practicable. The law applies to both

the public and private sectors, requires that any collection or use be for a lawful purpose, forbids the collection or re-use of personal data for a new purpose without the consent of the data subject, attempts to ensure that data collected is accurate, creates a system for individuals to gain access to data held about them, and so on. However, there are broad exemptions in the law for matters related to crime and security, meaning there is nothing stopping the police from creating dossiers on individuals based on the information they acquire.

Those engaged in political protest have seemed increasingly conscious of the potential for surveillance under this framework. In 2014, protestors began to use an "off-grid" mesh messaging app that did not rely on any service provider. In the anti-extradition bill protests of 2019, protestors used Apple's AirDrop feature to share plans in a decentralised way and left money on top of mass transit ticket machines so people did not have to use a traceable "Octopus" card. Protestors also tried to destroy "smart lampposts" they believed were tracking their movements. During the Covid pandemic, some residents refused to use the Government's "LeaveHomeSafe" contact tracing app, believing its real purpose was to track residents for non-health reasons. It is notable that there has never been any evidence provided to support the fears regarding either the lampposts or the tracing app – the opposition symbolises a

breakdown in trust between a portion of the population and the Government. The events of 2019 also led to perhaps the most significant change to Hong Kong's legal environment since the "handover" – the introduction of the National Security Law (NSL).

The NSL

Relying on its overall "supervisory jurisdiction" and referring to "acts of secession, violence, and terrorism that jeopardised national sovereignty and territorial integrity", in 2020 the National People's Congress inserted the NSL into Annex III of the Basic Law (national laws only apply to Hong Kong if they are added to Annex III). The NSL is wide-ranging in its scope. Not only does it create the offences of treason, subversion, sedition, and collusion with foreign entities as referred to in Art. 23 of the Basic Law, it provides a partially separate legal process for their investigation and prosecution. There are newly created dedicated national security departments in the Police Force and the Department of Justice, and NSL cases are heard by a selected panel of judges appointed by the Chief Executive. The most serious offences can even be removed from the Hong Kong legal system entirely and shifted to the Mainland, to be heard under Mainland law before Mainland judges. In terms of law enforcement powers related to surveillance and intercept, in some ways the NSL returns Hong Kong the pre-ICSO period

– in the context of detecting, preventing, or prosecuting national security offences, the Chief Executive may directly order the intercept of communications or covert surveillance of any individual if they feel it is necessary and proportional. The Commissioner for Interception and Surveillance has no oversight over these authorisations, and the authorisations are not legally reviewable.

The introduction of the NSL does not completely displace the local government's obligations under Art. 23 of the Basic Law, and more specific laws will be introduced on the subject. A new anti-doxxing law has already been adopted and a "fake news" law may be next. Depending on their specific application, both may have significant consequences for speech and the flow of information. The budget for the police force has also been dramatically increased since 2020, and the need to fight "local violent extremists" and combat "domestic terrorist activities" has been part of the justification. Hong Kong is now in a period where the understanding of "national security" seems increasingly co-terminus with "public order"; as a consequence, it is reasonable to also expect increased surveillance of the population in various forms.

There is likely to be little judicial opposition to this. The Court of Final Appeal has already accepted that the NSL itself is not subject to constitutional review for compatibility with the Basic Law, and I suspect the Court will be deferen-

tial to new legislative provisions if they are described as related to national security matters under Art. 23 of the Basic Law. While over the last twenty years both the people and the courts have shown some willingness to resist privacy intrusions, the rapid and significant changes consequent to the introduction of the NSL suggest this is less likely in the short-term future. While 9/11 may not have immediately triggered the expansion of the surveillance state in Hong Kong in the fashion that occurred elsewhere, the arc of the law is clearly now bending in that direction.

Anushka Jain and Vrinda Bhandari

The Development of Surveillance Technology in India

Beyond Judicial Review or Oversight

The Mumbai terror attack of 26 to 29 November 2008 ("26/11") is etched in the minds of Indian citizens, who can never forget the loss of life and destruction they witnessed in those three days. However, it was only one of the numerous attacks that took place in 2008 throughout India, which saw a total of 2400 attacks during the period of 2001-07. They culminated in serious questions being posed about the complete failure of the Indian internal security apparatus to pre-empt the attacks.

Despite a steady increase in terrorist activities in India since the 1980s, India's security apparatus was not robust. In the wake of these attacks, India resolved to strengthen it, which gave rise to various initiatives such as the National Intelligence Grid (NATGRID), the Centralised Monitoring System (CMS), the Crime and Criminal Tracking System (CCTNS), as well as the most recent National Automated Facial Recognition System (which is still being developed), with an aim to facilitate better coordination between the intelligence and law-enforcement agencies.

Even though India had seen a multitude of terror attacks in the 2000-08 period, 26/11 was the ultimate wake-up call to radically overhaul the surveillance architecture. However, the manner in which these changes were put in place calls into question the separation of powers and accountability mechanisms for the Indian government. The Executive, through orders, has put into place invasive systems

which do not have provisions for judicial review or oversight. This absence of oversight raises concerns about potential illegal mass surveillance, as well as the constitutionality of these systems themselves.

Developments in India's internal security in the aftermath of 26/11: Executive changes

In the aftermath of the 26/11 attacks in Mumbai, the then Minister of Home Affairs Mr Chidambaram made a statement in the lower house of the Indian Parliament, stating, "there is a need to make intelligence gathering and intelligence sharing more effective and result oriented". To fulfil this need, under Chidambaram, India started developing multiple surveillance technology projects post-2008, all of which suffer from the danger of "function creep". "Function creep" occurs when information is processed for a purpose that is not the originally specified purpose for which it was collected. This is because all these projects were authorised through executive action, with minimal transparency and without any legislative backing. In the absence of any legislation or parliamentary oversight mechanism, these mass surveillance systems could easily be misused to surveil Indian citizens illegally. Such misuse would then ultimately result in violations of the rights to life and liberty, freedom of speech and expression, freedom to assemble and to protest, as well as the right to privacy.

One of these systems is the National Intelligence Grid, better known as NATGRID, which was first conceptualised in 2009. NATGRID is an integrated intelligence grid that aims to leverage information technology to connect approved User Agencies (security/law enforcement) with designated Data Providers (Airlines, Banks, SEBI, Railway, Telecom etc.), to enhance the country's counter-terrorism capability.

NATGRID aims to use artificial intelligence and big data analysis to detect patterns from the massive amounts of data it will be collecting, and to provide real-time and even predictive analysis to the User Agencies. Essentially, the project has the capability to carry out 360-degree surveillance of Indian citizens. Such sweeping surveillance is violative of the Supreme Court of India's decision in K.S. Puttaswamy v. Union of India (2019, the "Aadhaar" judgment), which struck down the mandatory linking of the biometric ID ("Aadhaar") with an individual's bank account. The Court held that "*there cannot be such a sweeping provision which targets every resident of the country as a suspicious person*" without any evidence of wrongdoing on their part. The Crime and Criminal Tracking Network System (CCTNS), also conceptualised in 2009, aims to connect police stations and intelligence agencies across the country to increase ease of access to police data, also suffers from a similar folly of allowing 360-degree surveillance, in the event that its data is shared with other systems such as NATGRID.

One of the most intrusive systems among these is the Network Traffic Analysis (NETRA) which is operated by India's Defence Research and Development Organisation (DRDO). NETRA is a surveillance software capable of performing real-time interception of internet traffic for certain predefined keywords such as "attack", "bomb ', "blast" or "kill". Needless to say, these are words which are in common use and not just limited to use by potential terrorists. Therefore, such overly broad interception would clearly violate the right to freedom of expression.

The constitutionality of these 360-degree surveillance mechanisms has been challenged before the Delhi High Court for, *inter alia*, creating a mass illegal dragnet surveillance system and failing the proportionality standard under the *Puttaswamy* (Right to Privacy) decision of the Supreme Court. However, no substantive hearings have taken place and the surveillance challenge is still pending before the High Court. This is unfortunate, especially considering that the mass surveillance programs were notified by the government without passing any laws or statutory amendments.

Developments in India's internal security in the aftermath of 26/11: Legislative changes

In addition to drastic changes made by the executive, there were also legislative changes. However, the cause of concern is that both the executive and legislative changes gave

unrestricted power to the executive, and failed to put into place sufficient judicial oversight provisions.

The existing surveillance architecture in India majorly comprises two legislations: the Information Technology Act, 2000 ("IT Act") (in conjunction with the IT Rules) and the Indian Telegraph Act, 1885 (in conjunction with Rule 419A of the Indian Telegraph Rules, 1951). After the 26/11 attacks, India saw the introduction of new provisions related to surveillance, specifically, S. 69 of the IT Act, which was inserted in the IT Act through an amendment in 2009. Sec. 69 gave authorities the power to intercept, monitor, or decrypt any information online through any computer resource when it was "necessary or expedient" to do so in the interest of national security, public order etc. Notably, S. 69 departed from pre-existing surveillance provisions under the Telegraph Act, by removing the requirement of meeting the preconditions of "public emergency" or "public safety" before authorising surveillance. It allows the Central or State Governments, or any officer authorised on their behalf to authorise the interception or monitoring or decryption of data under certain circumstances. Similarly, S.5 of the Indian Telegraph Act allows the Central or State Government or any officer authorised on their behalf, to intercept or detain messages transmitted through a "telegraph" (or phone calls) on the occurrence of a public emergency or in the interest of public safety. These provisions fail to put

into place any effective oversight mechanism, which would allow for accountability of the executive issuing orders for surveillance, and to protect civil liberties.

These developments mirrored the developments post 9/11 in the US, which also carried out illegal surveillance of its citizens, through the President's Surveillance Program ("PSP") or "STELLARWIND". Over time the consensus has solidified that these laws facilitated mass violations of civil liberties in the name of national security. STELLARWIND was ultimately uncovered through the actions of the whistle-blower Edward Snowden and led to some reforms in US surveillance architecture.

The oversight process established under both the Indian IT Act and the Telegraph Act eschews judicial oversight in favour of executive oversight by setting up a three-member "Review Committee" comprising three top bureaucrats – the Cabinet Secretary, the Law Secretary, and the Telecom Secretary. The Review Committee is tasked with periodically reviewing the interception orders passed by the competent authority and assessing their validity. Thus, the IT Act and the Telegraph Act do not provide for any judicial, parliamentary, or independent oversight mechanism over electronic surveillance, whether at the *ex-ante, ex-post*, or the review stage. In addition, India's premier intelligence agencies – the Research & Analysis Wing (for external intelligence) and the Intelligence Bureau (for internal intelli-

gence) – exist outside any statutory framework and are thus, exempt from any independent oversight.

This stands in stark contrast to other major democracies, such as Germany, UK, and South Africa, where some form of parliamentary or judicial oversight over surveillance action exists. The European Court of Human Rights has also stressed the importance of judicial oversight in cases of secret surveillance. Even in the United States, the intelligence agencies are held accountable through Congressional Committees, Permanent and Senate Select Committees on Intelligence. The US government has also put in place a judicial oversight mechanism for authorizing surveillance against foreign nationals under the Foreign Intelligence Surveillance Act (FISA) courts, although the secrecy embedded in the FISA system leaves a lot to be desired.

In the absence of any inter-branch oversight, unbridled and disproportionate power is vested in the Indian executive. This impacts the horizontal separation of power between the executive, legislature and judiciary as envisaged under the Constitution of India and opens the door to the possibility of overbroad and illegal surveillance being carried out. Since surveillance, by its very nature, is carried out in secret, remedies for persons placed under illegal surveillance are effectively curtailed. As the recent Pegasus allegations reveal, in most cases, such individuals will likely not be aware, and will not be able to prove that they are un-

der surveillance in the first place. This violates the requirements of fairness and due process under Article 21 of the Constitution of India, as well as the broader requirements of natural justice. Thus, as one of us has argued before, an independent system of review *within* the surveillance framework is essential to protect the rights of the large number of people who will not be able to seek judicial redress against surveillance orders.

This becomes even more important given the lack of procedural guarantees within the existing surveillance framework. As per publicly available data, the central government issues approximately 7500-9000 telephone interception orders per month. This means that the Review Committee, which meets every two months, has an "unrealistic task" of reviewing 15,000-18,000 interception orders at every meeting. It is evident that it is almost impossible for the three-member Review Committee to ensure due process or application of mind on each surveillance request.

Thus, even the functioning of the executive oversight mechanism undermines the procedural safeguards laid down by the Supreme Court in *PUCL* (1997), which had upheld the constitutional validity of interception under the Telegraph Act. In fact, the lack of judicial oversight and the demonstrable inadequacy of the procedural safeguards have led to fresh challenges to the surveillance framework in India. Building on the proportionality argument recognised by

the Supreme Court in the famous privacy case, *Puttaswamy v Union of India* (2017), these petitions have argued for striking down Section 69 of the IT Act and Section 5(2) of the Telegraph Act. Although pleadings are complete, the matter is yet to be listed for final arguments.

Conclusion

The biggest limitation of the surveillance framework in India is the wide mandate and relatively unchecked power given to intelligence agencies, without adequate oversight and accountability mechanisms to protect civil liberties. These problems are compounded by the complete unwillingness of the government to improve transparency within the system. In recent years, the Ministry of Home Affairs of the Government of India has denied right to information requests (similar to FOIA requests in the US) seeking aggregate information about the total number of surveillance orders issued in a year or has claimed that such records and information have been destroyed per extant rules. Another cause of concern is that India still does not have a data protection law in place, and thus citizens do not have any statutory rights to the privacy of their personal data. However, the proposed Personal Data Protection Bill, 2019, which is currently before a Joint Parliamentary Committee, authorises the government to completely exempt law en-

forcement agencies from the ambit of the Act, and in the process, misses the bus on surveillance reform.

It is unlikely that any changes in the surveillance framework will come through legislative reform, especially given the relative "normalization" of surveillance activities during the COVID-19 pandemic. Interestingly enough, in 2020, US Courts partially ruled against two programs, which targeted email repositories and phone call logs which grew out of STELLARWIND, declaring them to be illegal in their present state, and finding them to have committed "widespread violations". One can only hope that the challenges to the statutory framework and surveillance infrastructure pending before the Supreme Court of India and the Delhi High Court respectively are decided soon and in a similar manner, and can usher in a new age of targeted, less-intrusive, and proportionate surveillance.

Nach den Anschlägen vom 11. September 2001 haben nur wenige politische Reaktionen so viel Aufmerksamkeit erregt wie die internationale Ausweitung staatlicher Überwachung und die damit einhergehende massive Verletzung des Rechts auf Privatsphäre. In dieser Publikation befassen wir uns mit der Normalisierung der Überwachung seit 9/11 und den Eingriffen in die Privatsphäre.