Twitter Thread by about:intel

about:intel
@aboutintel

With just a few days left in a turbulent year, we are looking back at some of the key discussions in European surveillance politics in 2020. A central theme were attempts to regulate & roll back existing, possibly undemocratic practices of industry & state security actors. (1/57)

One of these practices is big-data or predictive policing, a method of algorithmic risk mapping that has increasingly been used by law enforcement departments around Europe. Concerns include limited effectiveness & reproduction of bias with a veneer of objectiveness. (2/57)

So is predictive policing really a good idea? What advantages does it bring? How does it sit with the right to presumption of innocence and civil liberties? We asked academics, politicians, police chiefs & business leaders these questions: (3/57)

https://t.co/PGPfWlQYuC

Jamie Grace (@SHULawCrim) argues that data-driven policing can only be as good as the data feeding it. To ensure high data reliability & make predictive policing fair & ethical, a code of practice for data analytics in criminal justice is needed. (4/57)

https://t.co/97TApISBdk

An independent ethics committee to mitigate the risk of bias is also endorsed by @ChrisToddWMP (@WMPolice). He says that with high quality data, predictive policing can be used for the public good & fight crimes like domestic homicide. (5/57)

https://t.co/JONeI0M5y4

.@neina_hh (Senior Advisor AI @Linksfraktion) disagrees: predictive policing is ineffective & not enough attention is paid to the ‘human factor’, i.e. the rights & competencies of people using ML systems based on insufficient data. (6/57)

https://t.co/vqIPit15gA

Richard Helson of @Chorusintel, a predictive policing software provider, concedes that law enforcement does have to ensure legitimacy through data integrity & ethical frameworks. But to not utilise data in policing would be a mistake, he says.

(7/57)

https://t.co/iQp1B29RQI

Yet, according to @FiekeJ (@DataJusticeLab), studies show that predictive policing doesn't work. Rather it stems from an interventionist & racialised notion of security; its appeal to law enforcement is due to how police departments are organised. (8/57)

https://t.co/bVsvSsFeOo

Another controversial practice of industry & state actors is the proliferation of surveillance tech to repressive regimes around the world. Despite stricter controls since 2011, European governments & corporations remain key suppliers in the global surveillance trade. (9/57)

With government oppression in the world continuing to (in part) be “Made in EU”, we asked: what are the regulatory options for ensuring that surveillance technology produced in Europe will not be used to assail fundamental human rights elsewhere? (10/57)

https://t.co/mgAnEDuelt

Mark Bromley (@SIPRIorg) argues that to make existing export control regimes - Wassenaar & the EU dual-use regulation - more effective, public reporting obligations & a more inclusive policy review & formulation process need to be established. (11/57)

https://t.co/ZTrblFUjQk

A craze for profits makes the surveillance trade a race to the bottom, warns @Edin_O (@privacyint). To counter this, Europe must improve export controls but also leverage its security partnerships to improve legal & governance standards worldwide. (12/57)

https://t.co/PQnlPpzx2P

Europe could also leverage its economic power to incentivise proper use, argues @kat_lampert (@snv_berlin), by putting respect for human rights at the forefront of trade agreements, not unlike the EU’s Generalised Scheme of Preferences (GSP). (13/57)

https://t.co/YMCwUTZ92g

Another contentious practice this year were surveillance-based government responses to Covid-19. There was great concern that the surveillance infrastructure (potentially) built & expanded to respond to a public health need would not be walked back once in place. (14/57)

We reached out to experts in the UK, Germany, France, South Africa, & on EU level to understand which changes to the legal framework, policy, & use of surveillance had been triggered by Covid-19 & whether these changes were necessary & legitimate. (15/57)

https://t.co/0856FTcgxU

Data-driven automated enforcement is too simplistic to deal with complex human behaviour, argues @Javierruiz (@OpenRightsGroup). He contends that radical transparency, trust, and participation are better ways to fight the pandemic. (16/57)

https://t.co/R1uSIwrkpF

China has been using Covid-19 to advertise mass surveillance. @frankeschoen (@snv_berlin) says: to escape its pull, Europe must stick to the principle of necessity & remember: blazing the trail is to get results with the least invasive measures. (17/57)

https://t.co/5nkBPM7Ndi

.@DuncanJane (@go2uj) shows that following civil society pressure before the crisis, South Africa issued surprisingly strong regulations for the use of location data for contact tracing, incl. purpose specification & a sunset clause (18/57)

https://t.co/kAlb0CWS0l

.@ale_paulus & @z_edian (@snv_berlin) criticise China for leveraging Covid-19 for cyber operations: intelligence agencies should practice self-restraint during the pandemic to strengthen their government's international leadership projects. (19/57)

https://t.co/LaiEORGa06

The GDPR, the Data Protection Directive, the ECHR, & the ECtHR delimit the use of exceptional powers against Covid for EU states. It is critical that they remain exceptions, Elspeth Guild (@QMSchoolofLaw) & Elif Kuskonmaz (@UoPLaw) argue. (20/57)

https://t.co/E8PzxX4tUM

Law enforcement & other security agencies are increasingly resorting to automated video-surveillance. They claim that the technology helps to reduce crime & increase public safety. But critics have long raised the alarm. (21/57)

They criticise that video-surveillance has been pushed by the surveillance industry without real public demand. They also point to all the problems AI itself is fraught with — racial biases, false positives, & algorithmic inscrutability, among others. (22/57)

The fundamental worry is that full-scale automated video-surveillance in public will create a point of no return, after which we will be unable to live anonymously & assert our essential civil rights, such as freedom of assembly or freedom of speech. (23/57)

With the spotlight usually being on how to regulate technology after it has already been introduced, we wanted to take a step back and ask: Do we even want to allow automated video-surveillance in public spaces? (24/57)

https://t.co/wc9gYhdcXw

Hell no, says @Bojan_Perkov (@ShareConference). Studying the case of Belgrade, he argues that we need to resist the total surveillance of urban public spaces for law enforcement purposes if we want to keep living in free & democratic societies. (25/57)

https://t.co/pg8q0zmait

.@thorsten_frei (@cducsubt) has a different take: if used to target crimes of a grave nature, limited to crime hotspots, & if high standards are observed to protect against discrimination, facial recognition can & should be used to prevent crime. (26/57)

https://t.co/XpUAoXFC19

Still, what should be avoided, in any case, is that facial recognition databases are established without parliamentary debate or scrutiny, says Niovi Vavoula (@QMSchoolofLaw). Yet, that is currently happening in the next Prüm framework. (27/57)

https://t.co/YxATn2ErSp

One of this year's most successful attempts to roll back existing, possibly unconstitutional practices of industry or state security actors was likely the lawsuit of @ReporterOG, @freiheitsrechte et al against the BND act of 2016 before the @BVerfG. (28/57)

The ■■ Constitutional Court ruled that key provisions in the current legal framework on the German foreign intelligence service (BND Act) are unconstitutional and that the Bundestag has until December 2021 to rectify a long list of deficits. (29/57)

The basic premise of the Court’s judgement was that the right to private communication and the right to press freedom under Germany’s Basic Law are rights against state interference that ought to extend to foreigners in other countries, too. (30/57)

Many legal, technical & political decisions that now need to be made are open questions in other countries, too, e.g the mandate for bulk collection, oversight requirements, the rights and protections afforded to non-nationals, or special protections for journalists. (31/57)

The German cabinet passed a draft BND reform bill in December 2020. Does it provide a rights-based, modern framework for foreign intelligence or will it only be a matter of time before this bill, like the last, will be squashed in court? (32/57)

https://t.co/J5Hwm6nkEp

.@PatrickSensburg (@cducsubt) says the bill goes too far. He worries about the additional hurdles it will introduce for the BND’s surveillance of foreigners, because they would hurt the service’s operational effectiveness & ability to cooperate. (33/57)

https://t.co/Jl05y3u4sv

But his colleague from the Parliamentary Oversight Panel André Hahn (@Linksfraktion) says it does not nearly go far enough, leaving gaping loopholes for military intelligence activities, foreign cooperation, etc, & further fragmenting oversight. (34/57)

https://t.co/wfValthWeF

.@lisdittmer (@ReporterOG) agrees. She says that without further revisions, the bill will harm foreign journalists & their sources. She urges the Bundestag to significantly revise the proposal to make it conform to the Court's demands. (35/57)

https://t.co/LVAUcJWiP1

Above focused discussion series, we kept checking in on intelligence law & practice around Europe & gave context to intelligence news in our Spotlight section, be it litigation, legislation, scandals, policy input, or investigative features. (36/57)

https://t.co/GSqPToCGPN

Here, too, we looked at a whole range of surveillance practices by industry & government actors which had either just come to light, were being publicly reviewed, insufficiently overseen, litigated in court, or had been litigated & now needed constructive proposals. (37/57)

After the @BVerfG decision on the BND Act, the ■■ Bundestag needs to overhaul current legislation & create proper surveillance oversight. @twetzling explains the ruling & stresses the opportunity for a European harmonisation of standards. (38/57)

https://t.co/lhcis7cwsN

The ■■ Grand Coalition's wants to expand the powers of the domestic intelligence agency BfV. @newsvieth & @dietricharlotte argue this plan has no basis in evidence & fails to provide effective judicial authorisations & data-driven oversight. (39/57)

https://t.co/hNlbz8i9Km

For France's upcoming Intelligence Act reform @FloranVadillo says algorithmic surveillance needs debating & current oversight gaps addressing. Yet, to strike a stakeholder balance, he thinks only light touches to the existing law are warranted. (40/57)

https://t.co/Dvy9uadnpO

Recent landmark judgements (#SchremsII & the ■■ @BVerfG ruling on foreign intelligence legislation) should now pave the way for common standards to better protect both fundamental rights & national security, @twetzling & @dietricharlotte argue. (41/57)

https://t.co/IQ9nvsdWJi

Not only must Palantir be kept out of Europe, says @SophieintVeld (@D66, @RenewEurope), it is high time for the EU to gain more technological independence. Only then can it defend & assert its status as the last bastion of privacy. (42/57)

https://t.co/e95Udb7GAO

.@BLeQuerrec (@laquadrature) analysed the AG's opinion in the retention & access to metadata cases at the #CJEU: the AG rejected bulk data retention schemes but was in favour of limited retention of and real-time access to data. (43/57)

https://t.co/vEWSIK1J0b

According to @BGrabowskaMoroz, unlike some other EU countries, Poland has no independent surveillance oversight & lacks procedural safeguards. @hfhrpl, @panoptykon et al appealed to the #ECHR over the unfettered surveillance apparatus in Poland. (44/57)

https://t.co/KMQgJmTQZY

For years MI5 knowingly mishandled data collected through surveillance & violated statutory safeguards. This shows that the safeguards & oversight system of the 2016 IP Act are little more than window dressing, @gouldingmeg (@libertyhq) argues. (45/57)

https://t.co/04IW74HFRu

Sam Johnston Hawke (@Reprieve) explained the legal challenge brought against a questionable MI5 policy authorising agents to commit crimes in the field & why the government needed to mandate clear legal safeguards now. (46/57)

https://t.co/QGPdNcVskn

The UK government did introduce legislation later this year but set no limits on MI5 powers to authorise crimes (47/57)

https://t.co/uv59ajMuGf

According to @jan_jirat & Lorenz Naegeli (@wochenzeitung) the #ClubdeBerne has been influencing European intelligence for decades, whilst evading the few legal & regulatory frameworks that exist on international intelligence cooperation. (48/57)

https://t.co/MPfR7dJyso

@EleChelioudakis (@Homo_Digitalis_, @CiTiP_KULeuven) is concerned about a surge of police & border management surveillance in ■■, which occurs often without clear regulation & transparency, incl. facial recognition experiments & drone usage. (49/57)

https://t.co/RP0uBTShDr

There is a worrying gap between high-tech intelligence techniques & low-tech and inefficient oversight processes. @newsvieth & @twetzling (@snv_berlin) present seven ideas for more effective data-driven intelligence oversight. (50/57)

https://t.co/YqbK2RV828

As conflict moves to the cyber realm, peace efforts must, too, says Annika Hansen (@ZIF_Berlin). She looks at the untapped potential of digital technology in enhancing the effectiveness of peace operations to manage complex crises. (51/57)

https://t.co/muKtM3ZnFQ

With Spain's new Digital Agenda announced in late July, @Jescorde argued that it had to learn from its flawed predecessor & think of security, the economy, & privacy as inextricably linked in a healthy European digital society. (52/57)

https://t.co/7IvwYHzZGG

.@didierbigo (@sciencespo, @warstudies) says Covid tracking apps are "technological solutionism", adding a political problem (an enlarged surveillance apparatus) without solving the underlying one: the lack of an effective public health strategy. (53/57)

https://t.co/T3G8x9tZ2z

François Thuillier argues that the "war on terror" transformed France from a universalist & secular to an anti-terrorist republic. This new narrative misjudged the complexities of the world & blurred the line between liberalism & authoritarianism. (54/57)

https://t.co/k6Qmgt7UYd

All of these important discussions were made possible by the many fantastic, voluntary submissions we received from all over Europe, & sometimes beyond. We owe a ton of gratitude to everyone who joined the conversation on intelligence, technology, and democracy. (55/57)

If you would like to contribute in 2021, please do not hesitate to contact us at info@aboutintel.eu. Please also get in touch if you would like to give us feedback or if you would like to suggest new themes that deserve more attention from your point of view. (56/57)

A warm thank you to you all. Happy new year. And may the vaccine be with you. (57/57)

Yours sincerely,
Jan-David Franke (@frankeschoen), Editor