Guest Editorial eucrim 4/2018

Giovanni Buttarelli

eucrim
European Law Forum: Prevention • Investigation • Prosecution

EDITORIAL

AUTHOR

Giovanni Buttarelli

European Data Protection Supervisor

CITE THIS ARTICLE

Buttarelli, G. (2018). Guest Editorial eucrim 4/2018. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2018-020

Published in eucrim 2018, Vol. 13(4) pp 189 – 190

https://eucrim.eu

ISSN:

Dear Readers,

Police work and the administration of justice in general would be impossible without the exchange of personal information. As a member of the Italian judiciary, I can personally attest to this. At the same time, when applying and enforcing the law, judges and the police must themselves operate within the law, including the law of data protection.

Until last year, there was no general EU standard on how data should be processed for judicial and law enforcement purposes. The new "Police Directive" (Directive (EU) 2016/680) now fills that void. Though not directly applicable, like its more glamorous counterpart – the GDPR, there are no loopholes in its provisions. The choice of a directive rather than a regulation reflects the special responsibility that remains at the national level for law and order and national security. The commitment of Member States to putting these safeguards into practice is an ongoing concern. The deadline for transposition of the Directive was 9 May 2018, i.e. two years after adoption. But (at the time of writing) only 15 Member States have transposed it.

Member States tend to respond to appalling – but thankfully infrequent and isolated – incidents like the attacks in Strasbourg on December 2018 with calls for new EU-wide security measures. The 2016 PNR Directive was one such measure. Yet, as with the Police Directive, the deadline for transposition of PNR passed in May 2018, with a mere three Member States having fully transposed the Directive into national law. The Commission was obliged to reprimand 14 Member States that had failed to communicate the adoption of national legislation. It should not be necessary for the Commission to expend scarce resources in infringement proceedings. Failure to meet legislative commitments damages the credibility of those who have called so vocally for urgent EU action.

Crime is a stigma – it signifies actions that are, by their nature, intended to harm individuals or society generally. Civilised societies rightly aim to prevent crime and hold accountable those found guilty of having committed criminal acts, including the most heinous, such as terrorism. By contrast, the movement or migration of individuals and families, sometimes of entire communities, for a multitude of unique reasons, is a recurring fact and facet of human history. Migration has never been a crime in a free and democratic society.

Over the last few years, however, we have witnessed a growing tendency to conflate crime – an undisputed social ill – with the movement of people, which is innate to human freedom. This is why granting the police routine access to migration databases and creating new IT systems with dual purposes call into question the rule of law in a free and democratic society – because all of us may at some point wish or be forced to move across borders. I fear that calls for "interoperability" – while potentially justifiable – are part of this trend. New IT systems with dual purposes are under construction, and the competencies of EU agencies in the ex-third pillar sphere are being extended. Once large-scale data systems are connected, they cannot be unconnected. These are not merely technical choices; they are political choices, with ramifications for tens of thousands of people for generations to come.

Europe's challenge today is to respond to the popular calls for stricter controls on movement across external borders without stigmatising and criminalising the people crossing those borders. Furthermore, where technology is involved – whether shared databases or the scanning of biometric information, which is among the most intimate data pertaining to an individual – the EU needs to exercise extreme vigilance to ensure that individual dignity is not degraded. This is especially true given that, in our increasingly volatile and unequal world, the most vulnerable people tend to be the ones most often subjected to monitoring and coercion enabled by digital technologies, such as big data analytics, profiling, and automated decision-making.

https://doi.org/10.30709/eucrim-2018-020

Now is the time for the EU to reflect on the resources needed for data protection governance of judicial and police cooperation in the coming years. In so doing, we must be guided by the ever richer and more comprehensive body of case law from the European Court of Justice – such as *Tele2 Sverige/Watson* (Joined Cases C 203/15 and C 698/15) and *Ministerio Fiscal* (Case C 207/16), which set parameters for lawful requirements by which to retain and access subscriber, traffic, and location data.

This will shape the last chapter of the tripartite programme of data protection reform outlined by the European Commission in 2013 – first the GDPR and the Police Directive, then the EU institutions (see the recently adopted Regulation (EU) 2018/1725), and lastly the former third pillar. If we are successful, far from adding another layer of complexity to the existing and proposed new systems, we will have brought simplicity and accountability to the governance of personal data processing, fit for the purposes of the post-Lisbon Treaty Union.

In the meantime, the lawful reach of the state into the now massive quantities of personal information accumulated by the private sector continues to be debated in national and European courts. In April 2019, it will have been exactly five years since the CJEU struck down Directive 2006/24/EC, requiring the indiscriminate retention of telecommunications data. But a sustainable settlement has yet to be found, although the legality of bulk interception of communications and communications data will now be considered by Grand Chamber of the European Court of Human Rights (the cases are the *Big Brother Watch and Others v. the United Kingdom* and *Centrum för rättvisa v. Sweden*).

Police and investigating magistrates must be able to access – and require the preservation – of information relevant to investigations and prosecutions within reasonable timescales. Within the EU, it should make no difference where the data is held. The proposed e-evidence Regulation attempts to do this, although we will need explanations of how this new proposal fits with the existing European Investigation Order, which has only recently been implemented and not yet evaluated.

The EU is attempting to set internal standards, particularly in the context of Council of Europe discussions on a Second Additional Protocol to the Convention on Cybercrime, while at the same time agreeing on norms with third countries, notably the U.S. in light of the Cloud Act. Where EU law enforcement aims to access evidence held outside the EU by non-EU service providers, third countries will expect reciprocating entitlements to access evidence held by EU companies.

Ultimately, privacy, data protection, and freedom of expression are each at stake in the proposal currently under consideration to harmonise rules for “hosting service providers” in order to prevent the dissemination of terrorist content through their services and to ensure its swift removal. Instructions from the competent public authority to the platforms should be clear and specific to avoid collateral interference with the rights of the vast majority of people who use these services and have nothing at all to do with terrorist activity.

A major challenge across the board is to ensure appropriate accountability for these actions: it should be up to the judiciary, rather than private companies, to ensure compliance of law enforcement orders with fundamental rights law. Legal certainty will require the compatibility of these rules with the data protection framework, including rules on definitions of terms like “data” and “evidence,” on the rights of data subjects, and on data security. Moreover, mutual legal assistance and prevention of terrorism should not be privatised; there needs to be democratic accountability for actions which affect the fundamental rights of individuals.

https://doi.org/10.30709/eucrim-2018-020

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union