transcrime
Joint Research Centre on Transnational Crime

UNIVERSITÀ CATTOLICA del Sacro Cuore

PERSONAL DATA PROCESSING BY LAW ENFORCEMENT: FINDING A ROUTE BETWEEN INVESTIGATION OPPORTUNITIES AND REGULATORY FRAGMENTATION

By Massimiliano Carpino, Adjunct Professor at Università Cattolica del Sacro Cuore; Legal, Ethics & Compliance Advisor at Transcrime

Processing personal data in the field of police and judicial cooperation in criminal matters has long needed to strike a balance between on the one hand, investigative needs, cooperation and information sharing by crime enforcement authorities and, on the other, the safeguarding of individuals' fundamental rights and freedom.

The increasing complexity and transnational nature of criminal conducts raises difficult questions for police forces in regard to the applicable jurisdiction and rules for the effective gathering of evidence.

The employment of technology can facilitate the commission of many crimes as well as the concealment of the identity of the perpetrators and the profits of crime. As such, it can be an obstacle to policing. At the same time, technology is also a great opportunity for both preventive and judicial policing.

As far as preventive policing is concerned, examples are the use of artificial intelligence, big data and real-time facial recognition algorithms in public spaces or the use of computer systems that perform valuation and/or predictive functions.

As regards judicial policing, technology helps in performing some of the activities involved in preliminary investigations, such as:

Wiretapping of telephone conversations, computer or electronic communications

Acquiring telephone or electronic traffic data

Inspecting and searching computer, mobile and other electronic devices

Seizing electronic data and digital information

It is therefore clear that European and national regulations put in place to protect natural persons with regard to the processing of personal data by law enforcement should interplay with the criminal procedure laws of each Member State. But in both cases, there is a regulatory framework that is still fragmented and not uniform, and often requires great efforts of interpretation in order to identify the rules applicable to a specific case.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 made an important contribution to the protection of natural persons with regard to the processing of personal data by competent authorities, and on the free movement of such data.

This Directive, also known as the LEA Directive (Law Enforcement Agencies Directive) covers operations performed by "*competent authorities*" for the "*prevention, investigation and prosecution of criminal offences*". It has certainly improved the previous regulations, which only applied to the cross-border processing of personal data and not – as now – also to the processing carried out by police and judicial authorities at national level.

However, unlike the General Data Protection Regulation (GDPR, a EU Regulation directly applicable to all EU Member States), the LEA is an EU Directive requiring transposition into national law by all EU Member States, which can lead to further substantive and procedural discrepancies among the various national legal frameworks.

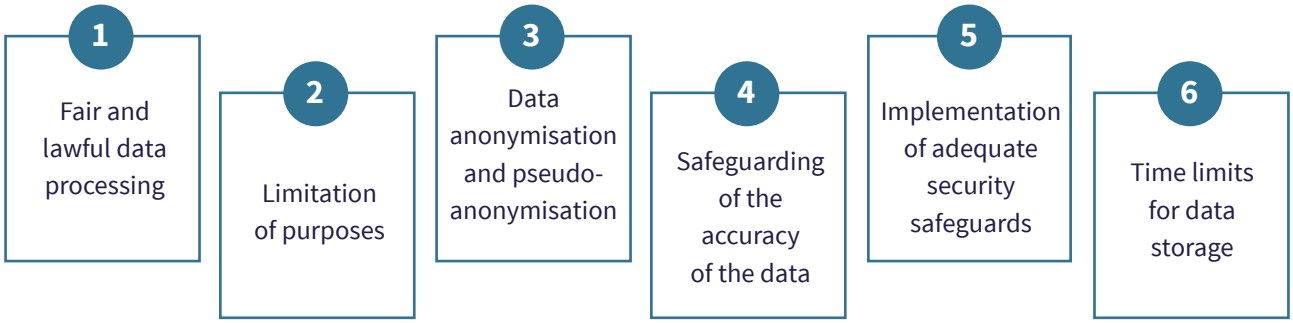
The regulatory fragmentation is evident if we consider that a law enforcement agency has to take account of both supranational laws governing the processing of personal data and, of course, all the relevant national laws, which in some Member States are snake pits difficult to be grappled with.

Among the regulatory pillars to be taken into account are the following:

- Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of personal data – 28 January 1981 – amended by Protocol CETS n° 223 and Protocol ETS n° 181;
- Recommendation R(87)15 regulating the use of personal data in the police sector;
- Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime;
- Regulation (EU) 2016/794 of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation (EUROPOL);
- Regulation (EU) 2018/1727 of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (EUROJUST).

Given the increasing importance of the issue, numerous police agencies have started to devote attention to the topic, and EUROPOL has created a specific Data Protection Function (DPF) led by a Data Protection Officer to carry out its daily tasks.

What is certain is that, when carrying out their work and as data controllers of a huge volume of personal data, both preventive and judicial police agencies must comply with the following principles:



All these principles apply both to data already collected (by the investigators themselves or by third parties) and to personal data collected during investigations.

In particular, it will be necessary for competent authorities to answer the following key questions:

- How are the databases in use being compiled? What are the sources of the data?
- Has the principle of privacy by design & by default been respected? Are the data accurate and up to date?
- Is the storage period justified by the purpose?
- Who can access the data, for what purpose, and when?
- Did we carry out a DPIA (Data Protection Impact Assessment)?
- Did we assess the risks of confidentiality, integrity and availability breach?
- Was the data processor (e.g. the private third party materially carrying out the wiretapping of computer or electronic communications on behalf of the data controller) selected only among those capable of guaranteeing technical and organisational measures appropriate to the risk? Does the data processor comply with the precepts of the laws?
- Are the requirements governing the transfer of data outside the European Union respected?

Transcrime (www.transcrime.it), the Joint Research Centre on Transnational Crime of the Università Cattolica del Sacro Cuore, is carrying out a number of research projects aimed at designing support tools for investigations by European competent authorities. Its spin-off Crime&tech (www.crimetech.it) is further developing and deploying them for operational activities.

At the same time, these projects represent an opportunity to exchange knowledge and experience with practitioners – law enforcement, anti-corruption authorities, judicial authorities, financial intelligence units – and find together a route through this fragmented regulatory environment which could increase the effectiveness and efficiency of investigative tools while respecting the fundamental rights of natural persons.

One of these projects is called DATACROS - Developing A Tool to Assess Corruption Risk factors in firms' Ownership Structures. It has been co-founded by European Union Internal Security Fund – Police. Its purpose is to develop a tool prototype to detect anomalies in firms' ownership structures that can flag high risks of collusion, corruption and money laundering in the European single market. The DATACROS tool has been designed exactly to follow and comply with all the principles listed above, and to provide law enforcement with an instrument to make investigations stronger.

Transcrime is the Joint research centre on transnational crime of the Università Cattolica del Sacro Cuore, the Alma Mater Studiorum Università di Bologna and the Università degli Studi di Perugia. The centre, directed by Professor Ernesto Ugo Savona, is based in Milan and has a staff of about 30 people, made up of academic researchers, contract researchers, Ph.D. candidates, interns and administrative personnel. Since its foundation, Transcrime has carried out more than 150 national and international research projects, mostly as coordinator.

CONTACTS

Transcrime

Registered office: Largo Gemelli, 1
Operational office: Via San Vittore, 43/45
20123 - Milano (Italia)
Tel: +39 02 7234 3715 / 3716

www.transcrime.it | transcrime@unicatt.it