Judicial investigation and data protection
The case of Cybercrime and e-evidence

Session 6: New Technologies as Means for and Tools Against Crime
XX Int’l Congress of Penal Law | Rome | 15 November 2019

Prof. Dr. Gert Vermeulen

t. +32 9 264 69 43
f. +32 9 264 84 94
Gert.Vermeulen@UGent.be
full-time academic

- international criminal law, EU criminal and JHA policy, cross-border police and judicial cooperation in criminal matters
- [other]

+25y working with/for (EU& MS) policy makers/police/judiciairies with data protection background

- BE: Privacy commissioner Belgian DPA
- EU: member SCG SIS II, Eurodac, VIS, CIS, Europol Cooperation Board, BTLE (Borders, Travel, Law Enforcement subgroup EDPB)
- CoE: T-PD expert (Consultative Committee Convention 108 + 2nd Protocol)
- ICDPPC: expert group enforcement cooperation
<table>
<thead>
<tr>
<th>level</th>
<th>existing/old</th>
<th>new/pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoE</td>
<td>R(87)15 use of personal data in the police sector</td>
<td>Protocol (CETS 223)</td>
</tr>
<tr>
<td></td>
<td>Convention 28 Januari 1981 (ETS 108)</td>
<td>draft 2nd Additional Protocol (e-evidence)</td>
</tr>
<tr>
<td></td>
<td>Additional Protocol 2001 (ETS 181)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2nd Additional Protocol 2001 to the MLA Convention (ETS 182) (Art. 26)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cybercrime Convention 2001 (Budapest) (ETS 185)</td>
<td></td>
</tr>
<tr>
<td>EU</td>
<td>Directive 95/46/EC</td>
<td>General Data Protection regulation (GDPR) 2016/679/EU</td>
</tr>
<tr>
<td></td>
<td>e-Privacy Directive 2002/58/EC</td>
<td>draft e-Privacy Regulation (lex specialis)</td>
</tr>
<tr>
<td></td>
<td>Data Retention Directive 2006/24/EG (annulled)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIS</td>
<td>Regulation 2018/1862 (police and judicial cooperation)</td>
</tr>
<tr>
<td></td>
<td>Decision 2007/533/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CIS</td>
<td>Regulation (EU) 2018/1727</td>
</tr>
<tr>
<td></td>
<td>Decision 2009/917/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Europol</td>
<td>Regulation (EU) 2017/1939</td>
</tr>
<tr>
<td></td>
<td>Regulation (EU) 2016/794</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eurojust</td>
<td>Regulation (EU) 2018/1727</td>
</tr>
<tr>
<td></td>
<td>Decision 2002/187/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EPPO</td>
<td>Regulation (EU) 2017/1939</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Swedish</td>
<td>Regulation (EU) 2019/816</td>
</tr>
<tr>
<td></td>
<td>Framework Decision 2006/960/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PNR</td>
<td>Regulation (EU) 2019/818 (police, judicial, asylum, migration)</td>
</tr>
<tr>
<td></td>
<td>Directive (EU) 2016/681</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prüm</td>
<td>Directive (EU) 2019/884</td>
</tr>
<tr>
<td></td>
<td>Decision 2008/615/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Decision 2008/616/JBZ</td>
</tr>
<tr>
<td></td>
<td>ECRIS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Framework Decision 2009/315/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Decision 2009/316/JHA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECRIS-TCN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interoperability</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MLA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Convention 29 May 2000 (Article 23)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Directive 2014/41/EU on the EIO (Article 20)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e-evidence</td>
<td>draft Regulation (production &amp; preservation orders)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>draft Directive (legal representatives)</td>
</tr>
</tbody>
</table>
EU
• “easy” to establish a compelling asymmetrical mechanism, including sanctions
• advantage of data protection coherence in the EU (market) bubble
• CONS reached a general approach on both the draft Regulation and Directive
• CONS also agreed to a double negotiation mandate for COM, with US (Cloud Act) and the CoE (2nd additional protocol) in June 2019
• whilst co-decision PE far from final | very critical LIBE report, release end last week
• covered also in session 8, be it not primarily from a data protection perspective

CoE | T-CY work on 2nd additional protocol Budapest Convention (world)
• purpose: to render traditional MLA under the Convention more effective
  • on direct disclosure by service providers of subscriber information
  • on giving effect to orders from another Party for expedited production of data
• multiple scenarios | within 108+ | 108+ to non-108+ | non-108+ to 108+/non-108+
• particular EU concerns (which do matter in a CoE context)
• T-PD(2019)8 | draft opinion on T-CY draft T-CY | next week T-PD Plenary: adoption
explanatory report (on pages 16-17, in point 4.2, para 4)

• “Information needed [in specific cases] for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time”

T-PD

• recognises that access to both static or dynamic IP addresses may be required in specific cases for the sole purpose of establishing the information as meant in Article 18.3 Budapest Convention

• stresses, however, that subscriber data should never be inclusive of any (other) traffic data or content data

• therefore recommends to specify under which circumstances IP addresses could be considered as subscriber information, as meant in Article 18.3 Budapest Convention

• can only support the potential inclusion of IP addresses under subscriber information if it is specified in the actual Protocol text (both in the articles on direct disclosure and traditional orders for expedited disclosure) and in the explanatory report that IP addresses are to be used solely for identification purposes and in specific cases only
T-PD equally recognises that some Parties currently treat dynamic IP address information as traffic data (for constitutional or other principled reasons) or as ‘access data’ (as a newly proposed category of data in the future EU Regulation on European production and preservation orders for electronic evidence in criminal matters)

• based thereon, T-CY has suggested, through the insertion of para 9.b of the draft text, to allow such Parties to reserve the right not to apply the provision on disclosure of subscriber information to “certain types of access numbers” (also reflected in the proposed explanatory report: “Accordingly, paragraph 9.b provides a reservation for some Parties”)

• T-PD regrets that the proposed solution leads to a fragmented regime for criminal cooperation and the protection of personal data, thus impacting the Protocol effectiveness

Re the full opt-out possibility (in point 9.a of the draft text) of the direct disclosure regime

• T-PD notes that, due to the fragmentation that is likely to arise from the variability of regimes, the “[high] expectations set for the new Protocol”, in that it “will need to stand the test of time in order to make a difference in terms of an effective criminal justice response with human rights and rule of law safeguards” may not be met

• If introduced at all, any new direct disclosure regime should be sufficiently straightforward and binding for all ratifying Parties, sustainably building on a common commitment to shared data protection conditions, safeguards or principles (infra)
Expedited production of traffic data

Explanatory report to paragraph 4 of the proposed text orders for expedited data production

• “under some Parties’ domestic laws, the production of traffic data may require further information because there are additional requirements in their laws for obtaining such data”

• T-PD questions the T-CY position that the only consequence thereof is that “additional information may need to be provided to the requested Party [...] in order to give effect to such order”

• T-PD finds the possibility of an opt-out from the regime as far as traffic data is concerned, as foreseen in paragraph 12 of the proposed text, equally insufficient

T-PD believes that

• the principled and historical distinction the Budapest Convention has made between measures relating to subscriber data vs. measures relating to traffic data, based on a difference in intrusiveness, should not be sacrificed for alleged reasons of efficiency
T-PD takes the position that

• a Protocol regime for disclosure of traffic data should, as a minimum requirement, allow for the combined data protection obligations of at least the Party of the requesting competent authority and the Party where the data subject was present whilst using the targeted service(s), if different from the requesting Party or the Party where the service provider is present

• as soon as it is possible to establish, based on the prior obtaining of subscriber data, where a person was while using any targeted service(s), it is key for the Protocol to make sure that the data protection, procedural and rule of law safeguards of the latter Party may be applied and complied with

  • in the case where that Party is the Party where the order originates from, such assurance is implied already, so that the Protocol may – only – then suffice allowing for the combined data protection obligations of at least the Party of the requesting competent authority and the Party where the service provider [or executing competent authority] is located

• the Protocol should contain specific provisions to guide Parties in case of conflict of laws, in that the laws offering the widest protection to the data subject will apply
Both the suggested direct disclosure and traditional cooperation mechanism pertain to the obtaining of data from service providers in another Party’s territory. The related draft explanatory report to both mechanisms reads as follows:

“[T]he term ‘a service provider in the territory of another Party’ requires that the service provider be physically present in the other Party. Under this Article, the mere fact that, for example, a service provider has established a contractual relationship with a company in a Party, but the service provider itself is not physically present in that Party, would not constitute the service provider being ‘in the territory’ of that Party. Paragraph 1 requires, in addition, that the data be in the service provider’s possession or control.”
T-PD insists that further clarification be added, ideally in the text of the draft articles themselves, if not at least in the corresponding parts of the explanatory report, on when a service provider will be considered ‘physically present’ in a Party’s territory

- against the back-drop of the significant jurisprudential contentieux in the past decade around jurisdiction over service providers abroad, in which a multitude of criteria (a range of ‘establishment’ criteria, ‘offering’ criteria etc.) has passed in review, the proposed two criteria (negatively: that a contractual relationship does not suffice; positively: that data must be in the service provider’s possession or control) seem insufficient to bring optimal clarity

- T-PD finds such clarity crucial in order for any future mechanism not to be undermined as well as to avoid forum shopping by authorities/Parties
  - unless mandatory common safeguards were to be incorporated in the Protocol
  - risk for undermining: multinational service providers may [still] be confronted with parallel orders issued to its establishments or branches in several jurisdictions
  - risk for forum shopping: authorities/Parties may opt to send orders to the jurisdiction of presence of the service provider where the lowest data protection standards apply

- T-PD sees relevance in adding more clarity, e.g. by stipulating in the Protocol or in the explanatory report that a service provider will be considered ‘physically present’ in a Party’s territory
  - when it has a stable infrastructure through which it actually pursues an economic activity for an indefinite period and from where the business of providing services is carried out or managed
The explanatory report to the envisaged article on disclosure of subscriber information clarifies that the “special procedural instructions” that need to accompany a disclosure order submitted to service providers are meant to “cover, in particular, any request for confidentiality, including a request for non-disclosure of the order to the subscriber or other third parties” and that “[t]herefore, in order to avoid the risk of premature disclosure of the investigation, Parties are encouraged to be aware of applicable law and a service provider’s policies concerning subscriber notification, prior to submitting the order under paragraph 1 to the service provider”

- T-PD requests reconsideration of the opening left for domestic laws or discretionary policies of service providers that would not guarantee the confidentiality sought
- reason: whilst confidentiality may be important to maintain efficiency in criminal investigations, it may equally be vital in safeguarding data protection
- T-PD favours the inclusion of a self-standing provision on confidentiality in the Protocol, for which it suggests inspiration is drawn from:
  - Articles 26.2 of the Budapest Convention (ETS 185)
  - Articles 27.8 of the Budapest Convention (ETS 185)
  - Article 25 of the Second Additional Protocol to the Convention on MLA in criminal matters (ETS 182)
Confidentiality [continued]

The explanatory report to the envisaged article on traditional orders for the expedited production of data clarifies that “[u]nder paragraph 3.c, the request should also include all special instructions, including for example requests for certification or confidentiality under Article 27.8 of the Convention, at the time of transmission to ensure the proper processing of the request”

• T-PD stresses that, from the draft T-CY text as it stands, it cannot be derived that Article 27.8 of the Budapest Convention applies in a Protocol context

• T-PD, consequently, stresses the importance that a self-standing provision on confidentiality be included in the Protocol itself, for both the direct and the traditional mechanism for obtaining information from service providers
importance of two-directional data protection conditions and safeguards

• since receiving entity may be either a competent authority (in case of traditional MLA or of direct, asymmetrical transfers) or a private data controller (service provider)

only three references in the explanatory report, exclusively targeted at “parties that have data protection requirements” (1-2) or would wish to limit or refuse cooperation based on “conditions and safeguards (including with regard to data protection)” (3)

• 1. only a reminder to parties having data protection requirements of their obligation under domestic laws to provide “a clear basis for the processing of personal data” by service providers in response to an order which they directly received

• 2. relates to int’l data transfers, without stipulating the actual safeguards that a service provider may require to be able to transfer “responsive subscriber information” (blank cross-reference to a future article on data protection, relying on “important public interest” (infra)).

• 3. “MLA is in principle to be extensive, and impediments thereto strictly limited”, so that “accordingly, conditions and refusals should also be limited in line with the objectives of this Article to eliminate barriers to transborder sharing of subscriber information and traffic data and to provide more efficient and expedited procedures than traditional mutual mutual assistance”

• T-PD considers that labelling data protection conditions and safeguards as potential ‘impediments’ and ‘barriers’ is inappropriate and does not reflect the balanced functioning of democracies safeguarding human rights and the rule of law. It is furthermore not in line with the case-law of the European Court of Human Rights. It believes – based on tangible experiences – that the efficiency of cooperation would be genuinely enhanced when embedded in a shared commitment to respect common data protection principles.
In claiming that the envisaged direct disclosure regime in the Protocol reflects an “important public interest” (supra), the T-CY proposal seeks to base the entire direct disclosure concept exclusively on the derogatory regimes of Article 14.4.c of Convention 108+ and, for the EU Member States, on Articles 49.1(d) juncto 49.4 GDPR.

- T-PD firmly disagrees with and opposes the envisaged structural and systemic reliance on derogations as a standardised means to allow for direct, asymmetrical transfer

preferred, straightforward and sustainable option: Protocol Parties accede to 108+

subsidiary options:

- incorporation in the Protocol (as a legally binding instrument between the Parties) of common mandatory data protection safeguards [list: infra point 7], grounded in, closely aligned with and consistently interpreted in line with Convention 108+

- building ETS 182, so as to ensure consistency with at least the CoE’s data protection acquis in the context of judicial cooperation in criminal matters

- leaving it to the competent authority or data controller of a Party to make the transfer of personal data conditional upon an appropriate level of data protection

- comparable with the optional regime as in Article 26.3, 2nd indent ETS 182, which would need to be rephrased as to ensure two-directional applicability, both in the context of direct transfers and transfers between traditional competent authorities
in the last subsidiary option (building on ETS 182), T-PD suggests, in view of enabling, ensuring, enforcing compliance by private data controllers with the Protocol’s data protection conditions/safeguards (public international law), to

• stipulate in the Protocol that if a data controller or competent authority of a Party requires an appropriate level of data protection in the receiving Party, such condition shall be considered to be met if “the receiving competent authority or data controller of the latter Party undertakes to process the personal data transferred subject to the conditions and safeguards under the domestic law of the former Party [i.e. the Party from where personal data would be transferred], including obligations the latter has undertaken under [Convention 108 and its Protocol] and/or other applicable bilateral or international data protection agreements guaranteeing the protection of individuals by the implementation of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+ [list infra point 7]” [para 25]

• combined data protection of at least the Parties of the requesting competent authority and the location of the service provider [or executing competent authority] [para 26]

• ex Article 14.3.b of Convention 108+ (“legally-binding and enforceable”), T-PD suggests an additional obligation for Parties to stipulate in their domestic legislation that violations of such undertaking by a receiving competent authority or data controller in their territory may give rise to all judicial and non-judicial sanctions and remedies available under their laws [para 27]
Use restrictions

whilst the draft articles on direct disclosure or traditional, expedited ordering of information limit the issuing of orders to information which is needed for the issuing Party’s specific criminal investigations or proceedings, the draft text remains fully silent on the purposes for which transferred personal data can be used by the receiving competent authority or service provider

• T-PD recommends to include explanations at least in the explanatory report on a commonly agreed distinction between data processing (including transfers) for criminal investigation purposes and those undertaken for national security purposes, in line with the Issue paper “Democratic and effective oversight of national security services“ published by the CoE Commissioner for Human Rights

• T-PD requests that clear use restrictions be inserted in the Protocol, applicable to both direct and traditional, expedited cooperation

• T-PD suggests to phrase such use restrictions based on Article 26 of ETS 182, amending them mutatis mutandis and extending them to also cover use limitations upon a private data controller (service provider) to which a request is transferred

• this could translate in three provisions, stipulating respectively that
Use restrictions [continued]

1. *[mutatis mutandis adaptation of Article 26.1 ETS 182]* personal data transferred by a competent authority or data controller of a Party *as a result of the execution of a request made under the Protocol* by a competent authority of the receiving Party, may be used by the latter only for:

   a. the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence within the scope of articles 14.2 and 25.1 of the Budapest Convention;

   b. other judicial/administrative proceedings directly related to proceedings under (a);

   c. preventing an immediate and serious threat to public security;

2. *[mutatis mutandis adaptation of Article 26.2 ETS 182]* such data may however be used by the competent authority for *any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject*

3. *[extension to cover use limitations for service providers]* the request received and the information it contains can *only* be used by the receiving data controller for the purpose of the execution of a request made under this Protocol.
In both subsidiary options (preferred option: Parties required to accede to Convention 108+), T-PD requests incorporation in the Protocol of at least the following safeguards, grounded in, closely aligned with and consistently interpreted in line with Convention 108+

a. purpose legitimacy, purpose specificity and purpose limitation;
b. lawfulness;
c. fairness and transparency;
d. necessity for and proportionality to the legitimate purpose pursued;
e. non-excessive data processing and data minimisation;
f. adequacy, relevance and accuracy of data;
g. data retention limitation;
h. accountability of controllers and processors;
i. logging, data security and data breach notification duty;
j. specific, additional safeguards for special categories of sensitive data;
k. lawful use of exceptions and derogations;
l. enforceable data subjects’ rights and effective administrative or judicial redress;
m. appropriate protection in (onward) data transfers;
n. free, specific and explicit consent where consent of the data subject is the legal basis [FN: specialty]
o. effective independent oversight
Monitoring effectivity of safeguards

T-PD

• stresses the importance of the effectivity of the data protection safeguards and ensuring that Parties to the Second additional Protocol effectively apply and enforce them in practice

• proposes that an evaluation of the implementation of the data protection safeguards be carried out, possibly relying on the findings and recommendations of the mechanism introduced in Article 4.3 of Convention 108+ for Parties to Convention 108+, and, for other countries, on Article 23.f of Convention 108+
www.ircp.org

Contact
Prof. Dr. Gert Vermeulen
t. +32 9 264 69 43
t. +32 9 264 84 94
Gert.Vermeulen@UGent.be
http://www.linkedin.com/in/gert-vermeulen-42b00068

IRCP
Ghent University
Universiteitstraat 4
B – 9000 Ghent