

Investigation and due process

A defence lawyer's view

Competition Conference

Best practice in investigations

RA MMag. Dr. Astrid Ablasser-Neuhuber

12 December 2014, Vienna

www.bpv-huegel.com

bpv HÜGEL



Defence Lawyer's Perspective



Selected questions

- **Level playing field for defence rights in investigations**
 - at all necessary?
 - anyway sufficient safeguards through human rights and general principles of EU-law?
- **New challenges by digital data and forensic “excitement”**
 - are existing defence rights still apt for the technological show down?
 - in particular: will they withstand new standards of transparency?

A level playing field for Europe?

- **Implementation of European competition law by Member States – key problem:**
 - substantive provisions for competition rules laid down in TFEU
 - >> direct applicability of Art 101 and 102
 - procedural aspects for investigations not harmonized
 - >> parallel competence EC-NCAs

Sufficient Safeguards?

- **Which guarantees?** (*selection relevant in particular with dawn raids*)

General principles of EU law	Charter of Fundamental Rights of the EU	European Convention on Human Rights
Principle of effectiveness	Respect for private and family life, Art 7	Right to a fair trial, Art 6
Principle of proportionality	Chapter VI – Justice, Art 47-50	(Nulla poena sine lege, Art 7)
Confidentiality of attorney-client relationship	Right to defence of Art 48 in conjunction with Art 41(2)	Right to respect for private and family life, Art 8

Sufficient safeguards?



Example Czech Republic: Recent judgment of ECtHR, dated 2 October 2014 (DELTA PEKARNY a.s., CNo 97/11).

- *prior court approval* and supervision by an independent body before an investigation or stronger and effective *ex post facto* control by independent court required by Art 8 ECRH (para 87)
- However, according to the decision, only 14 of the EU member states have the obligation to obtain prior court approval when performing antitrust dawn raids (para 57, referring to the EC *Investigative Powers Report*)
- Note: perhaps another lesson to learn – also the “*dérroulement*” - the actual execution of the dawn raid is covered by the judgment (para 87 and 90ff)

Sufficient safeguards?



Example Austria: Recent decision of the Higher Administrative Court (Bundesverwaltungsgericht), 15 October 2014 (W134 2000196-1)

- Fishing expeditions (eg by taking copies of entire share drives and entire mailserver) are admissible since the authority “...*may also search for information sources, which are not yet known.*”
- Based on standing case-law by the ECJ (referring to **Roquette Frères** of 22 October 2002, Case C-94/00, paras 54 and 55 and the case-law cited therein), the GC reminds in **Nexans** (14 November 2012, T-135/09) that
 - fishing expedition not admissible: The EC can only examine product areas in which it has “*reasonable grounds*” to suspect an infringement (para 43)
 - and finds it “*incompatible with the protection of the sphere of private activity of legal persons, guaranteed as a fundamental right in a democratic society*” (para 65)
- GC in **Deutsche Bahn** (6 September 2013, T-289/11, para 139, et al): Exhaustive search (e.g. of an office) only if there are reasons to suggest that it may yield relevant evidence, some (rather light) judicial control exercised over keywords (= no copying of entire file share),

Sufficient safeguards?

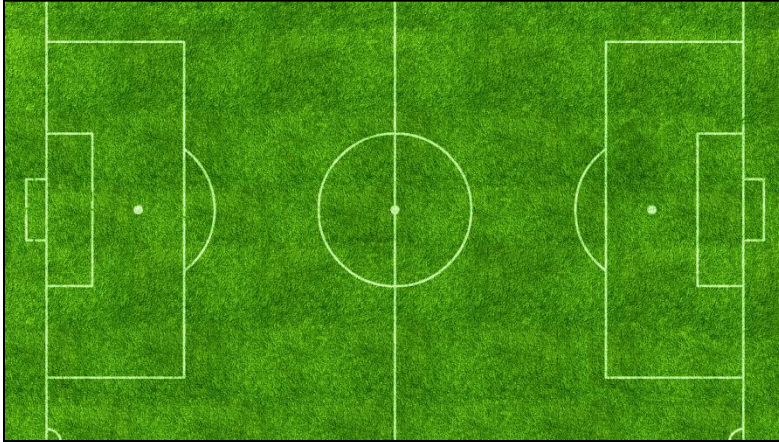


Example Germany and Austria:



- ECJ in **AM&S v Commission** (18 May 1982, C-155/79) and **Akzo Nobel Chemicals v Commission** (14 September 2010, C-550/07P)
 - Protection of the correspondence with external lawyer (legal professional privilege), clear scope of legal professional privilege, for example not even a “*glance*” may be made at those documents
 - based on the principle of observance of confidentiality (*AM&S*, para 18; *Akzo*, para 69)
 - In Austria and Germany, legal privilege - with minor exceptions - not recognized

A level playing field for Europe?



*the frame & the game is
the same*

**it still feels somehow
different..**



Technological challenges

Digital data and forensic hype



Technological challenges

■ New toolbox:

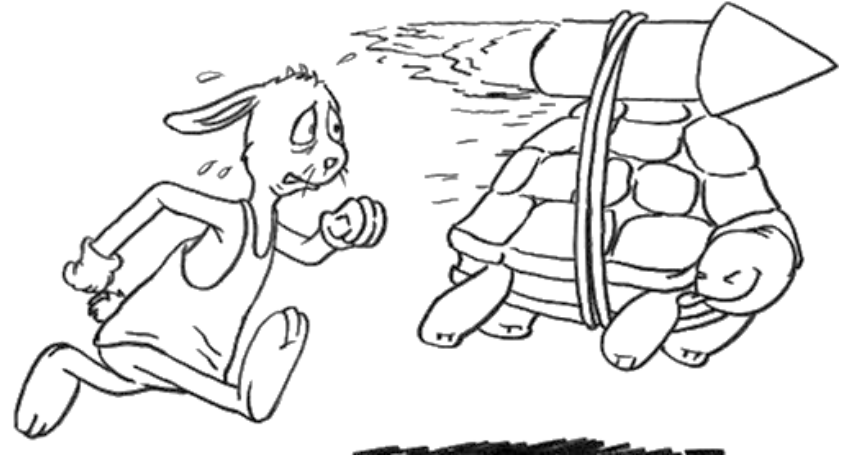
- digital data is in the focus of the investigation
- effective **forensic IT tools** (including eDiscovery platforms) in order to copy, search and duplicate data are in place
- capacities to copy vast amounts of information onto a tiny device
- temptation to collect all available information, **lock, stock and barrel**

Technological challenges

- **The question is how to safeguard existing defence rights (and obligations under data protection law)**
 - sheer mass of data volume
 - Great difficulties to check electronic data (not printed out) as to whether they are covered by the search warrant or not
 - lack of parallel forensic capacities (it is not always a global player which is raided) on site
 - No level playing field as regards concrete handling

Technological challenges

Defence rights lag some way behind technological progress.



- **this might be in conflict with the**
 - right to respect for private and family life
 - principle of proportionality
 - right to protection of data

Technological challenges

- **Problem clearly intensified through** parallel development towards more transparency because of (wider) access to the files for third parties by
 - New Directive on certain rules governing actions for damages under national law for infringements of the competition law (published as Directive 2014/104/EU in OJ 2014/L 349 /1 on 5 December 2014)
 - EU Transparency Regulation
 - National provisions on transparency
 - Relaxation of the official secret

Technological challenges

- **Exemptions from access to file?**
 - usually only for business secrets (apart from leniency and settlement declarations according to the new Directive on actions for damages)
 - Additional problem - different definitions of business secrets throughout the European Union
- **In general no defence available** for data which is neither business secret, nor leniency or settlement declaration; data not covered by the search warrant does not fall under these categories

Technological challenges

- Thank you very much for your attention

Contact

**MMag. Dr.
Astrid Ablasser-Neuhuber**
Attorney-at-Law
Partner

Contact:
bpv Hügel Rechtsanwälte OG
Donau-City-Straße 11
1220 Wien
Phone: +43 1 260 50-205
Fax: +43 1 260 50-208
e-mail: astrid.ablasser@bpv-huegel.com