

**Workshop on Botnet Detection, Measurement,
Disinfection & Defence**
Cologne, 09. March 2011

Legal Guide on Technical Approaches against Botnets

Ivo A. Ivanov
Attorney at law, General Corporate Counsel
eco Association

Agenda

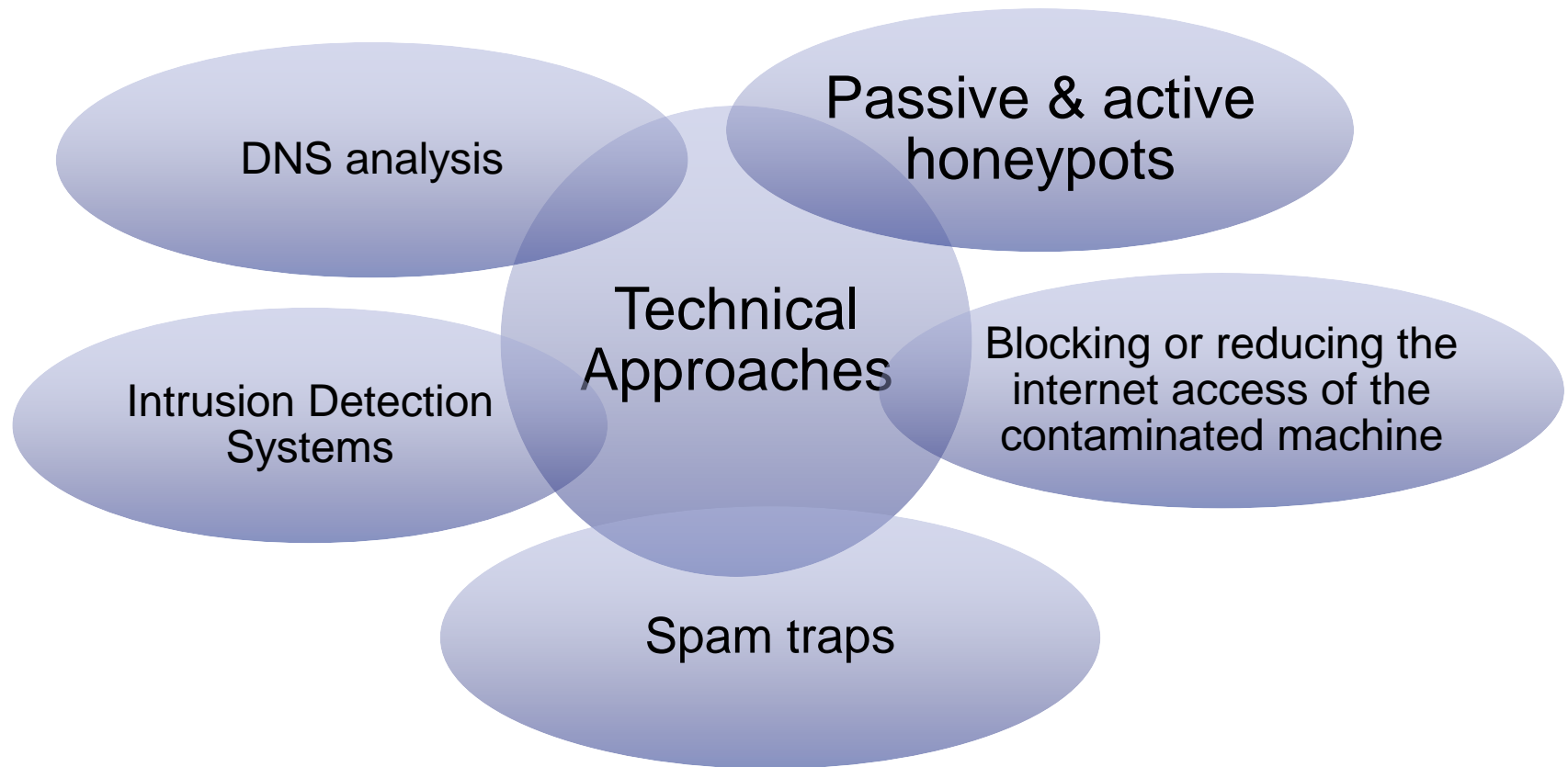


**Data collection
and processing
within technical
approaches
against Botnets**

**Does the data
collection and
processing
reflect the data
protection and
telecom law ?**

**Justifications and
Permissions**

Different Technical Approaches against botnets



Collecting and processing of information & data

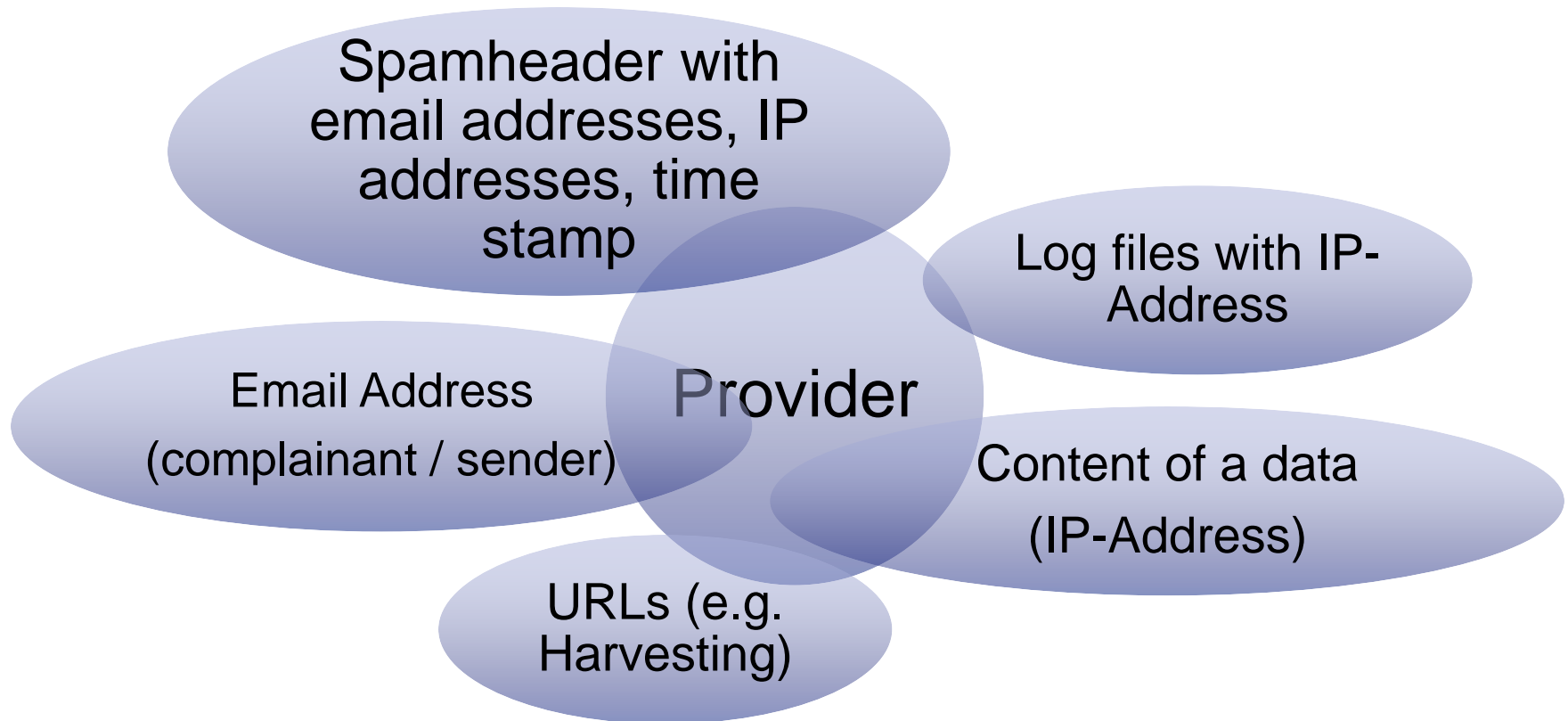
I. Collecting of information

- Analysing the traffic on the network / email traffic
- Analysing of firewall logs
- Abuse complains
- Analysing of websites and websites visits

II. Providing of information to third parties

- Providing of traffic and customer data to third parties (e.g. other providers)

Type of information & data



Types of Data from the perspective of the Provider

Traffic data

- Any data processed for the purpose of the telecommunications process
- e.g. IP-Address, email address etc.

Customer Data

- Any data processed for the purpose of a contractual relationship between the Provider and the customers
- e.g. name, address, bank account etc.

Traffic & Customer data protected by:

Secrecy of telecommunications

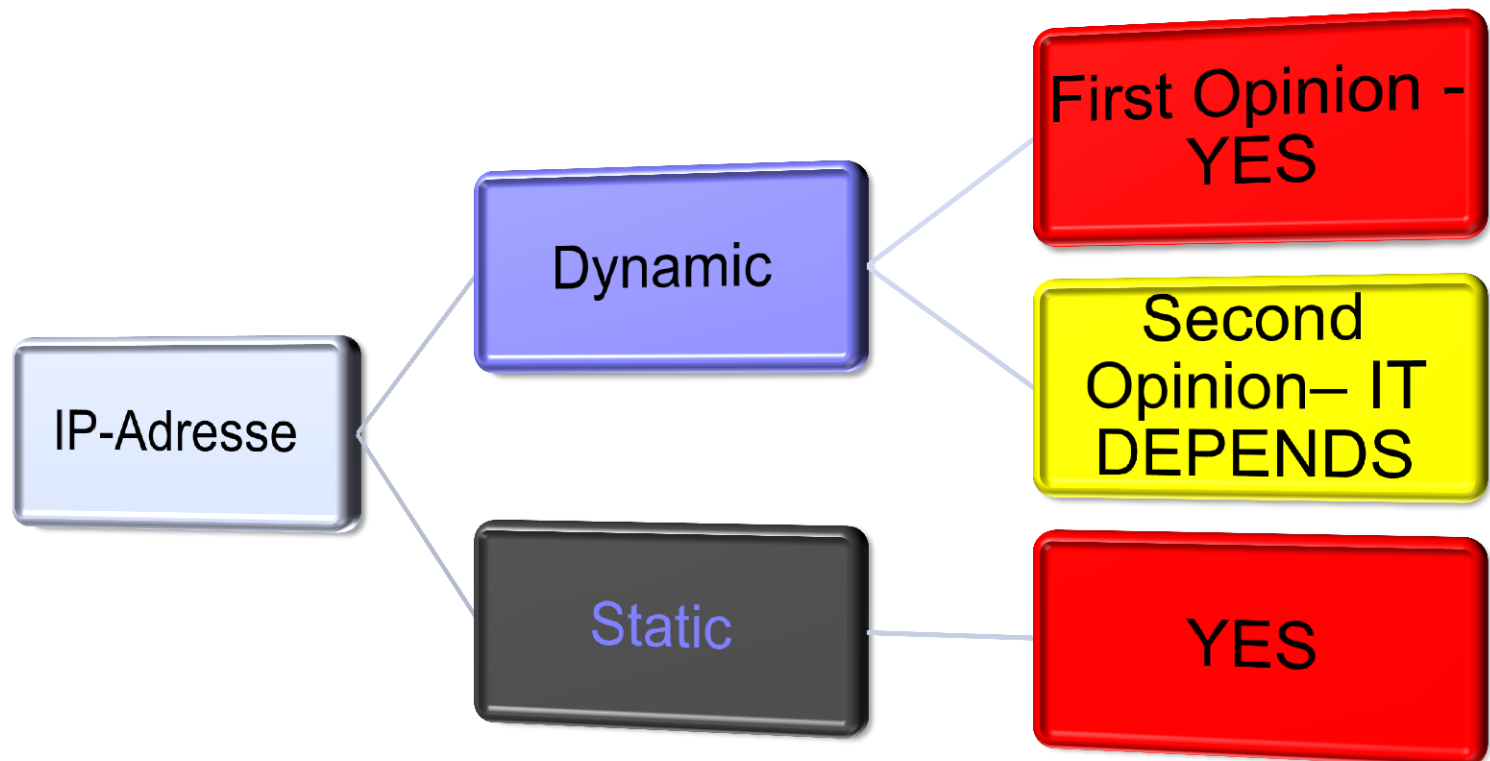
- Protects the customer of operators of telecommunications services
- Protects the content and details on the telecommunication process (Who? With whom? How? How long?)
- Protection during the transmission and as long as the customer does not control the process

Data protection law

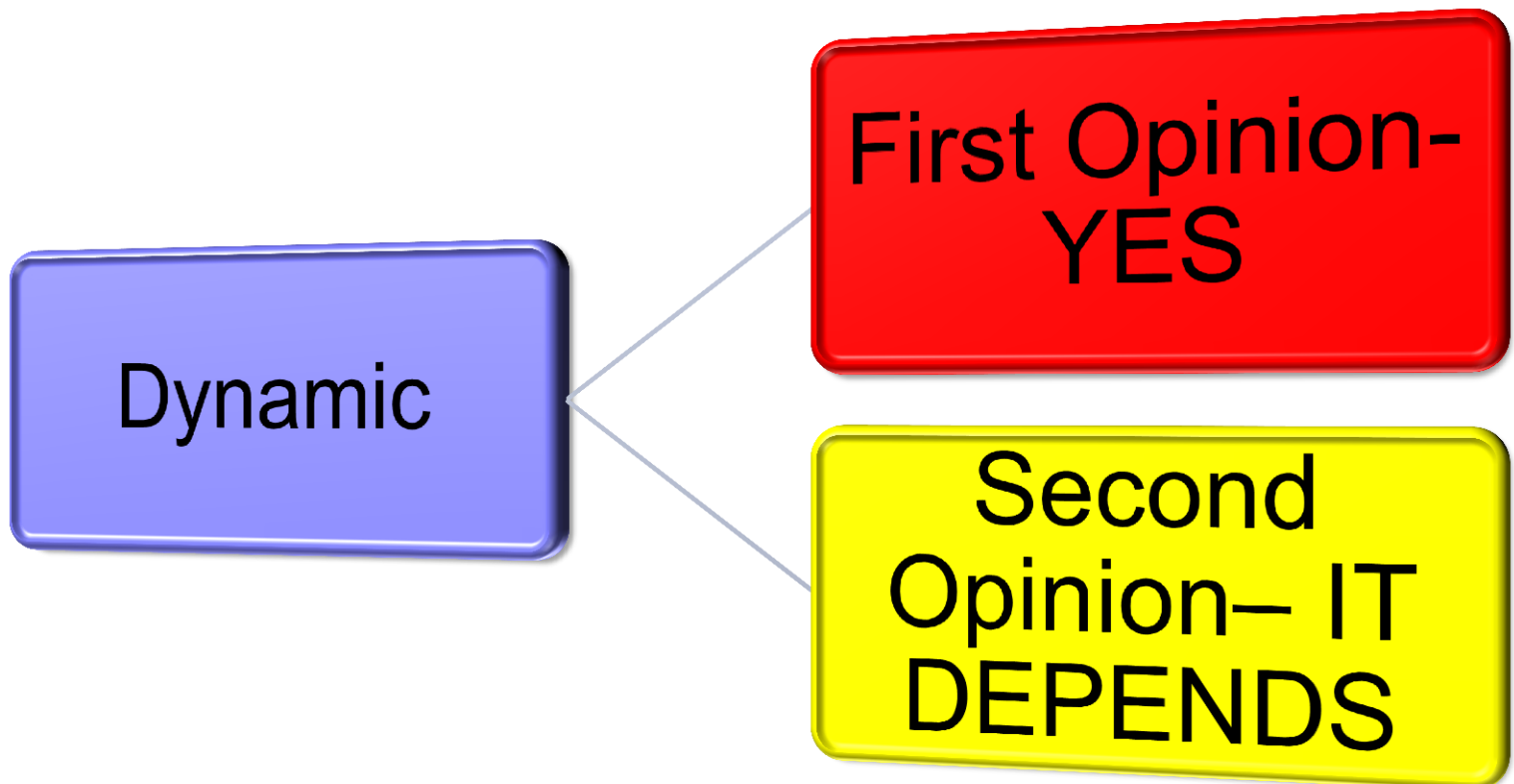
- Protects data that relates to a living **individual** who can be identified
 - from those data, or
 - from those data and other information which is in the possession of, or is likely to come into the possession of the Data Controller.
- Data within a telecommunications process that relates to a corporate (§ 91. Paragraph 1 sentence 2 TKG)

IP-Address – Personal Data ????????

IP-Adress – Personal Data?



IP-Adress – Personal Data?



IP-Address – Personal Data?

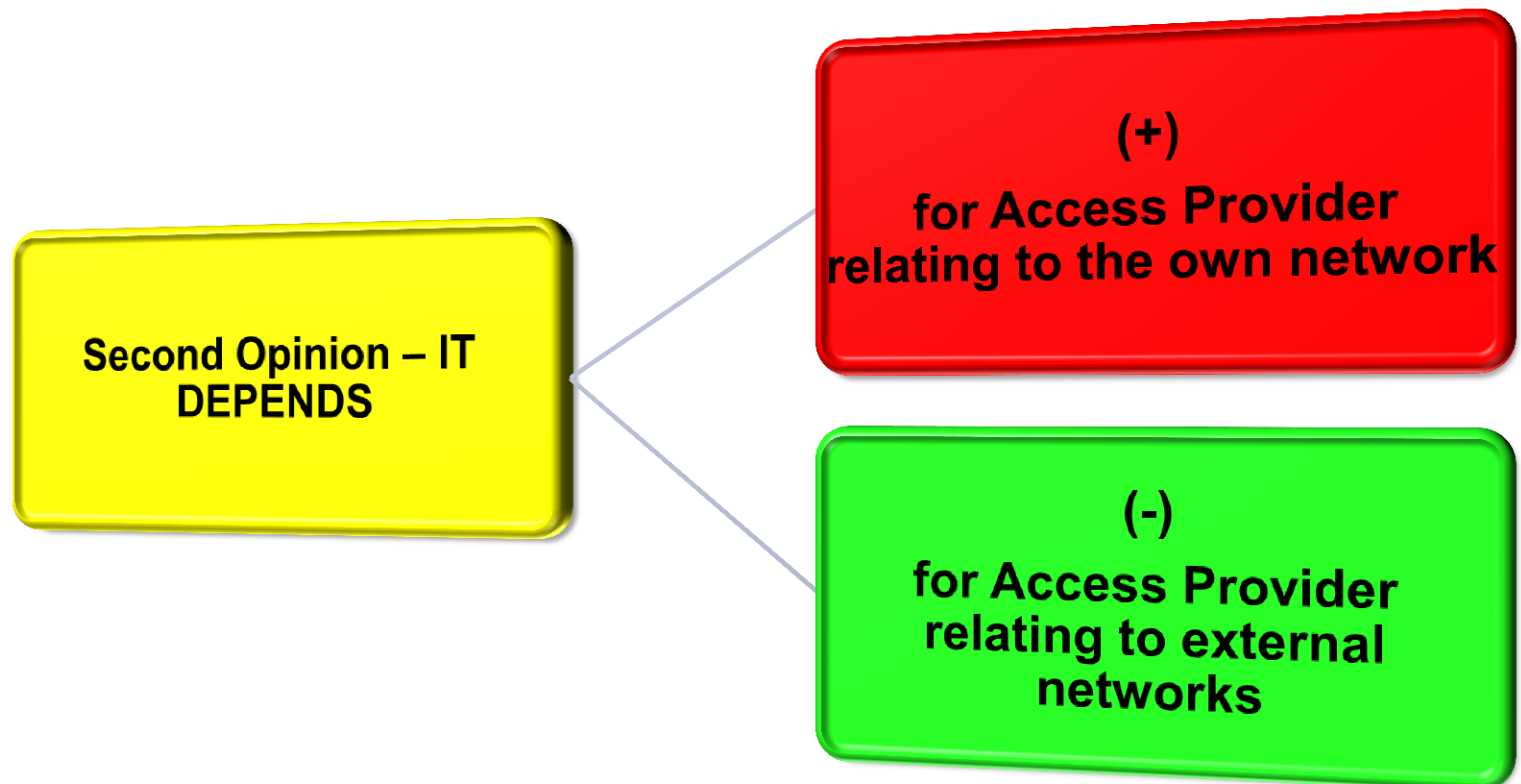
First Opinion- YES

- AG Berlin, VG Wiesbaden
- Concurrence Opinion in the Professional Law Literature
- The Data Protection Authorities (Peter Schaar EU - Art. 29-Group)

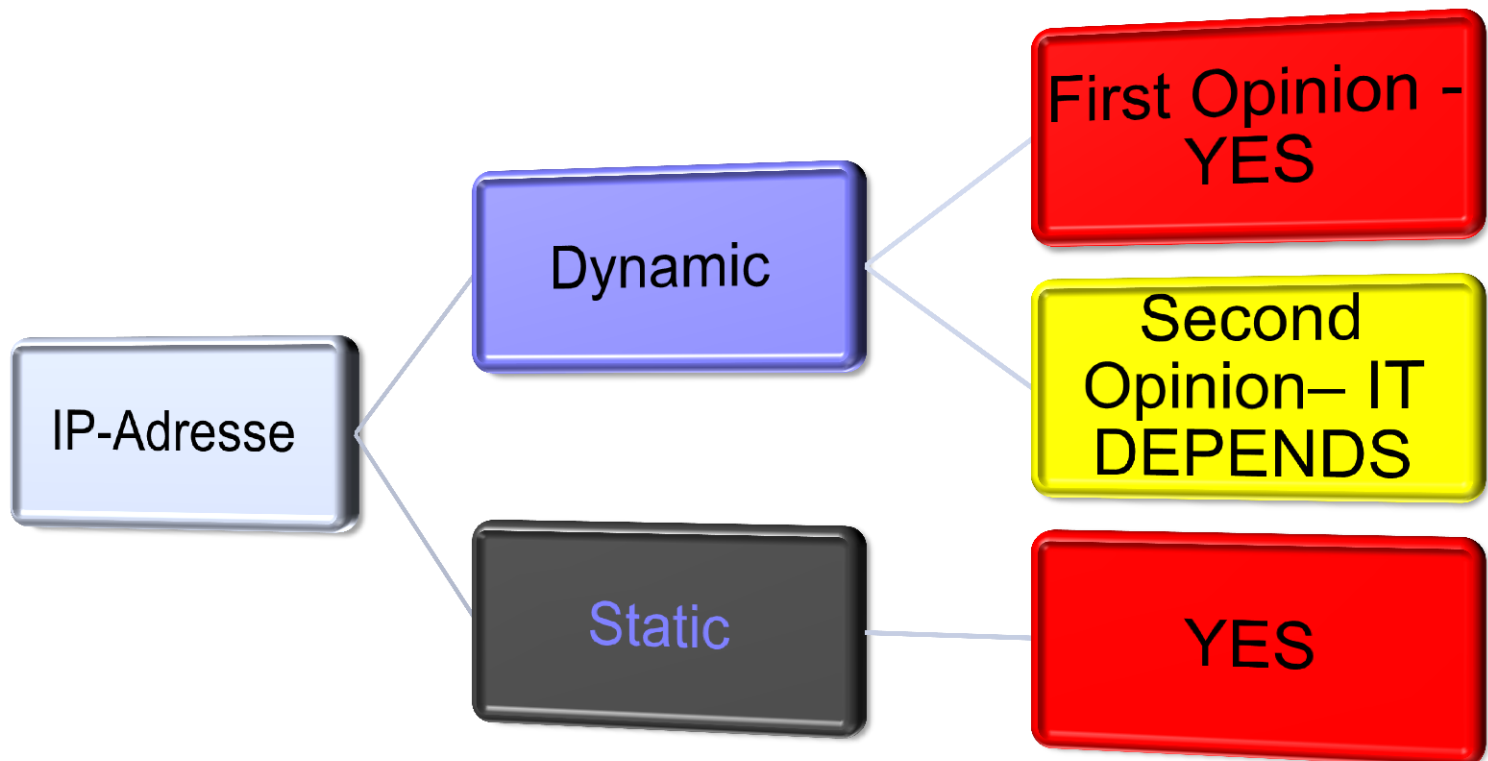
**Second Opinion – IT
DEPENDS**

- AG München, AG Frankenthal
- Concurrence Opinion in the Professional Law Literature

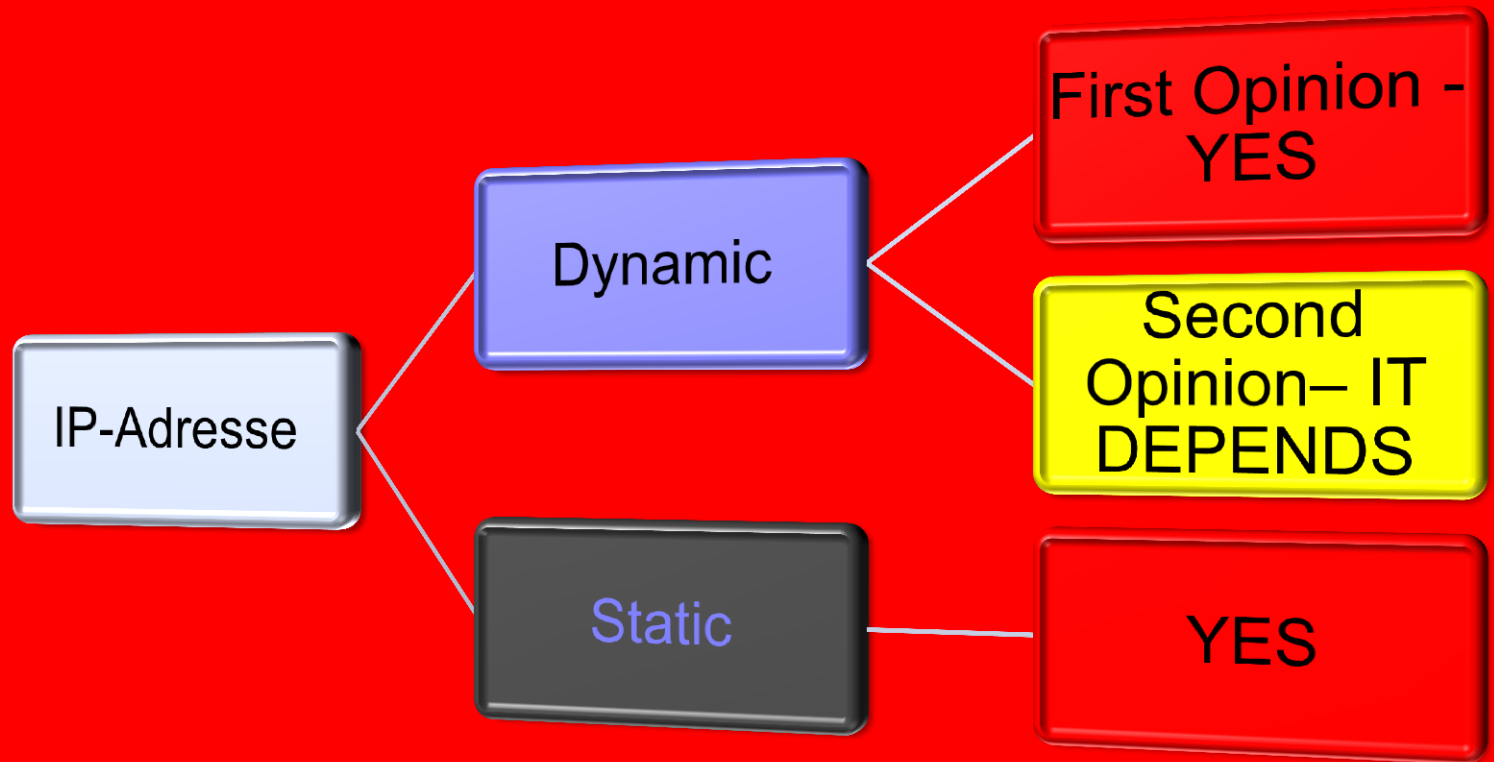
IP-Address – Personal Data?



IP-Address – Personal Data?



IP-Address – Personal Data?



Traffic & Customer data protected by:

Secrecy of telecommunications

- Protects the customer of operators of telecommunications services
- Protects the content and details on the telecommunication process (Who? With whom? How? How long?)
- Protection during the transmission and as long as the customer does not control the process

Data protection law

- Protects data that relates to a living **individual** who can be identified
 - from those data, or
 - from those data and other information which is in the possession of, or is likely to come into the possession of the Data Controller.
- Data within a telecommunications process that relates to a corporate (§ 91. Paragraph 1 sentence 2 TKG)

Traffic & Customer Data protected by the Criminal Law (Strafgesetzbuch StGB)

§ 202a StGB – Data Espionage

- Whoever, **without authorization**, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.....

§ 202b StGB – Phishing

- Whosoever **unlawfully** intercepts data (section 202a (2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment of not more than two years or a fine...

§ 206 StGB – Violation of Secrecy of Telecommunications

- Whoever, **without authorization**, makes a communication to another person about facts which are subject to postal or telecommunications confidentiality and which became known to him as the owner or employee of an enterprise in the business of providing postal or telecommunications services, shall be punished... with imprisonment for not more than five years or a fine.

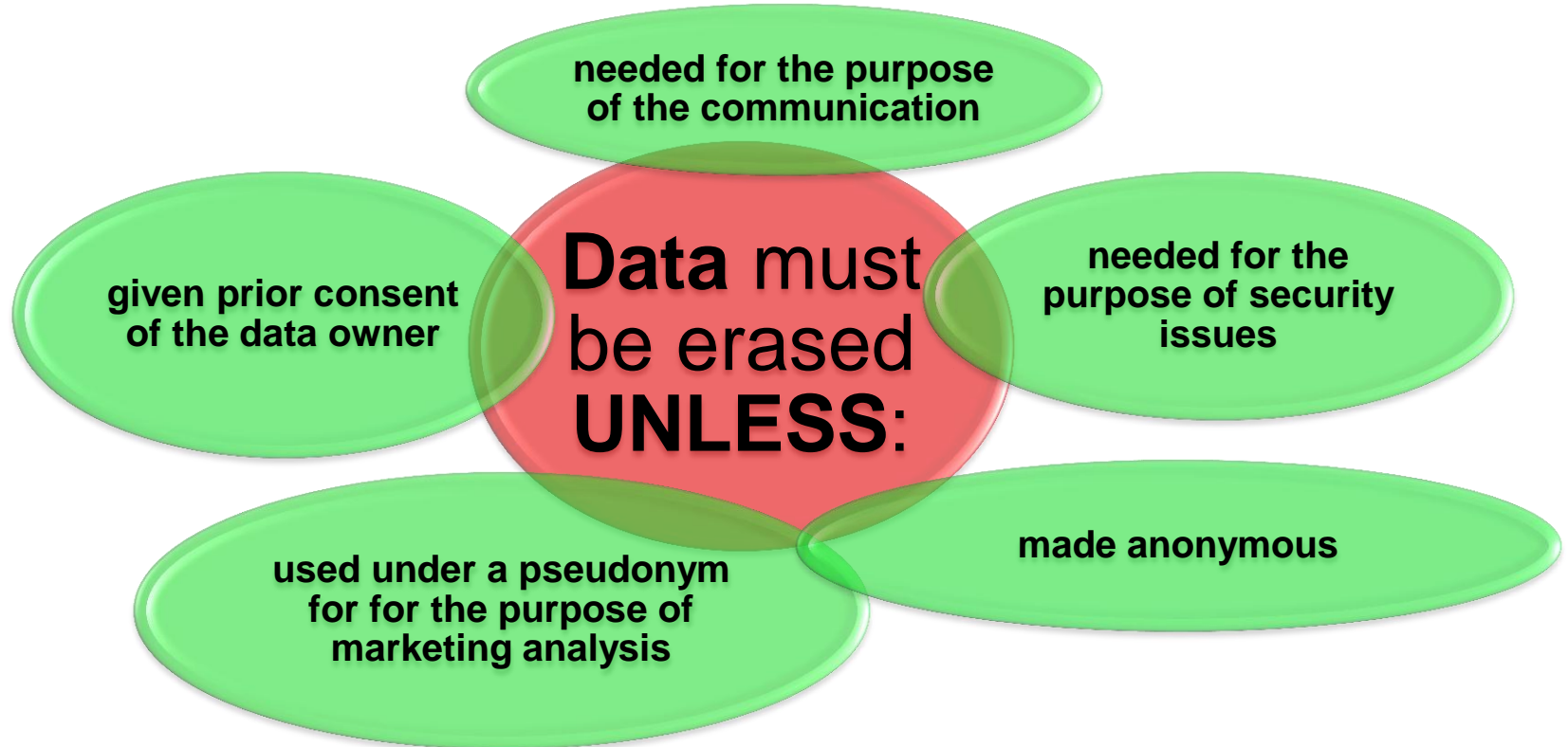
Important Legal Justifications for Anti-Botnet measures

Telecom Law

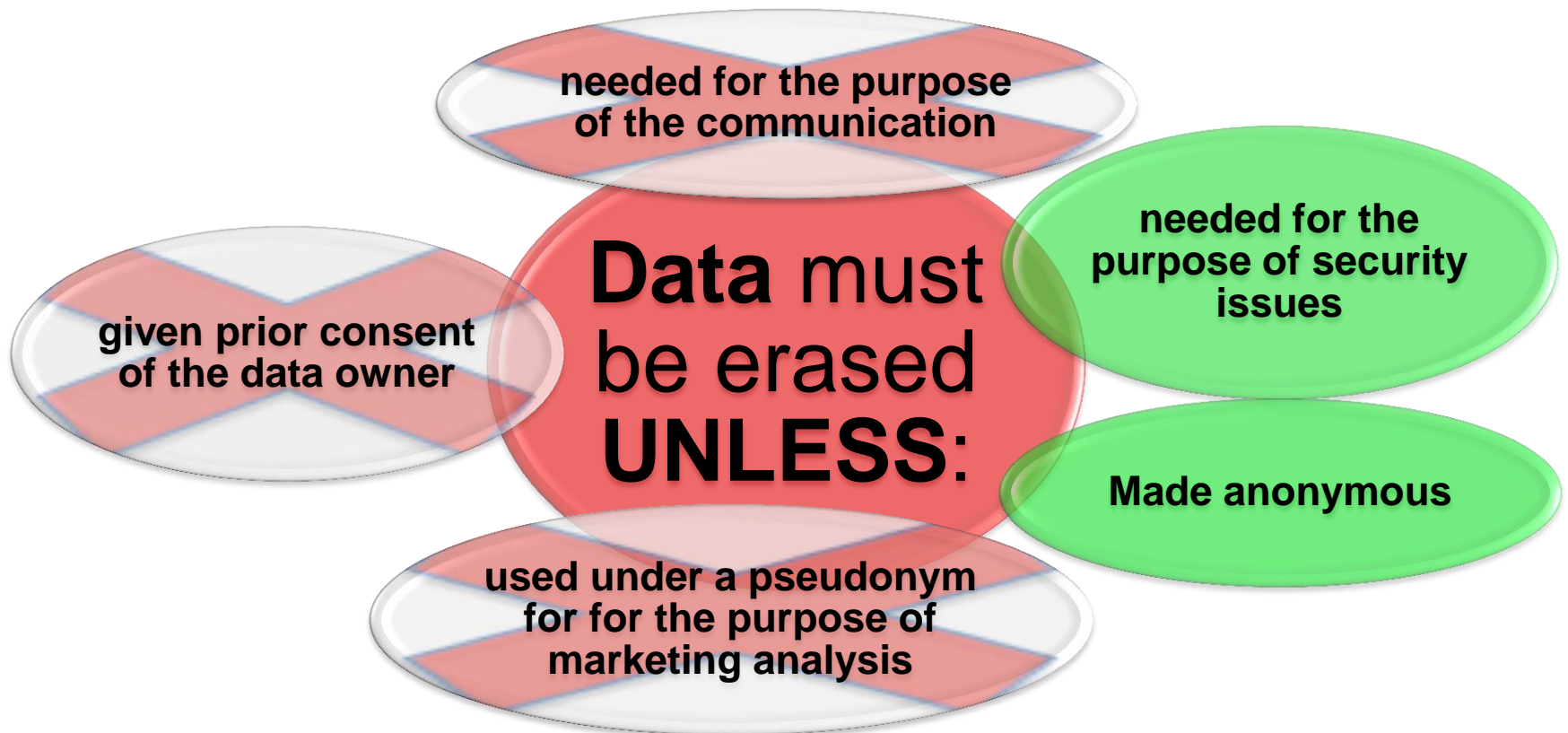
General Data Protection Law

Contract Law

Legal Premises for the Processing of Traffic & Customer Data by the Telecom Law



Legal Premises for the Processing of Traffic and Customer Data by the Telecom Law



Processing of traffic & customer data needed for the purpose of security issues – § 100 German Telecommunications Act (TKG)

**Where required, the Provider may collect
and use the traffic & customer data need to:**

**detect and put a stop to the unlawful use
of telecommunications networks and
services**

**detect, locate and eliminate faults and
malfunctions in
telecommunications systems.**

**from the total traffic
data not more than
six
months old**

**concrete reasons
to suppose that
unlawful use**

**for reasonable
period / case law:
7 days without any
concrete reason**

**erase, when not
anymore required**

General Data Protection Law (BDSG)

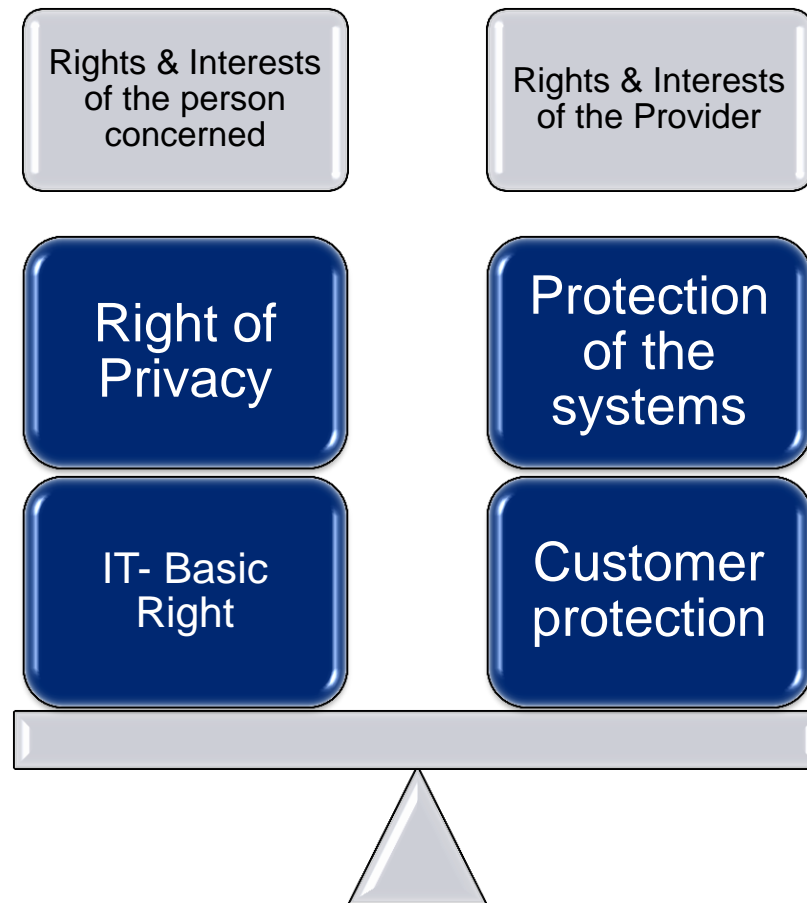
§ 28 Abs. 1 Nr. 2 BDSG

- The storage, modification or communication of personal data or their use as a means of fulfilling one's own business purposes shall be admissible...
- in so far as this is necessary to safeguard justified interests of the controller of the data file and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use.

§ 28 Abs. 2 Nr. 2 a) BDSG

shall be admissible...in so far as this is necessary to safeguard justified interests of a third party

Weighing of interests



Contract Law (German Civil Code – BGB)

§ 242 BGB Performance in good faith

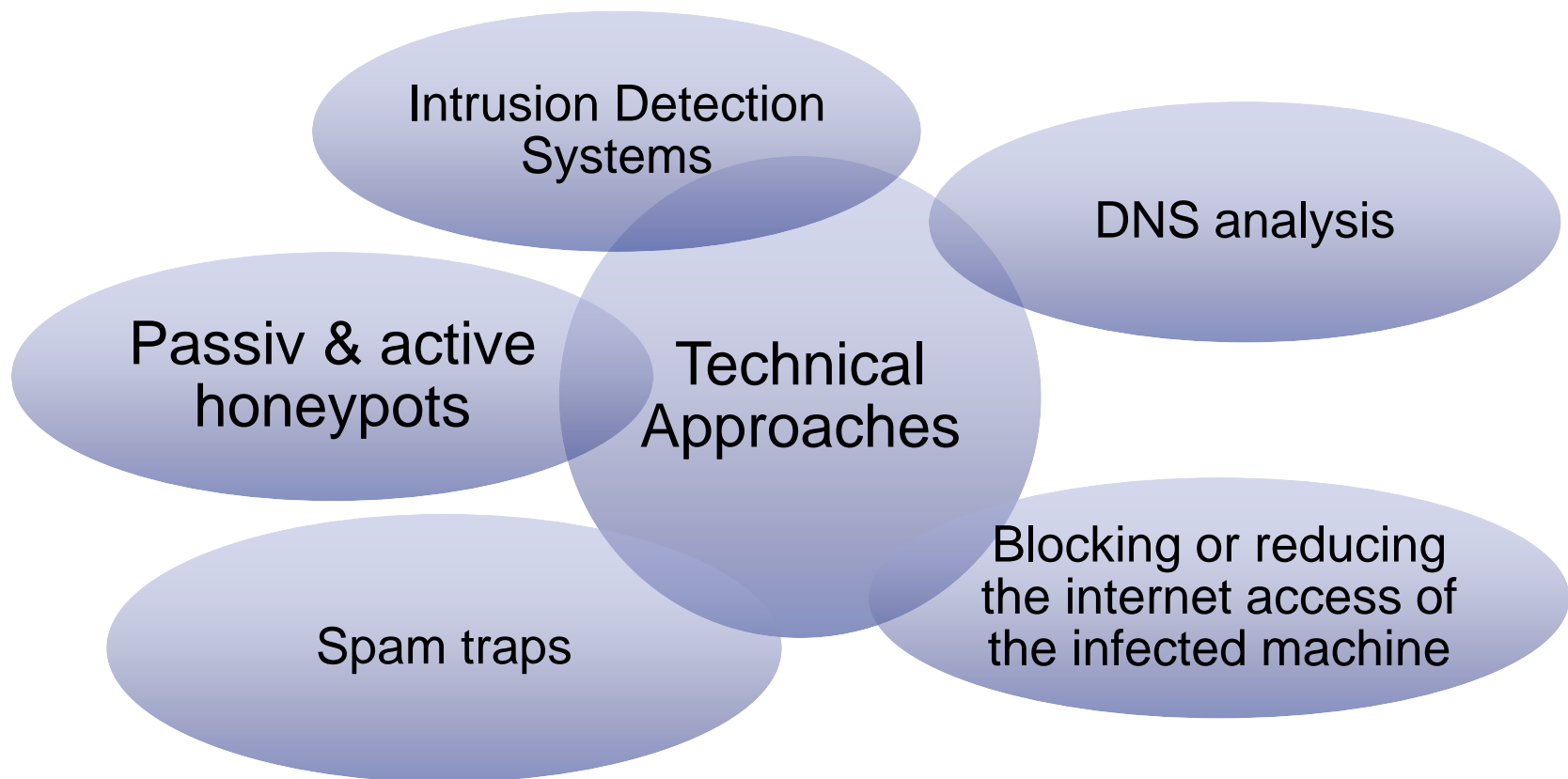
- duty to perform according to the requirements of good faith, taking customary practice into consideration.

§ 314 BGB – Termination, for a compelling reason

- Each party may terminate a contract for the performance of a continuing obligation for a compelling reason without a notice period.
- There is a compelling reason if the terminating party, taking into account all the circumstances of the specific case and weighing the interests of both parties, cannot reasonably be expected to continue the contractual relationship until the agreed end or until the expiry of a notice period.

Specifications in the General Terms and Conditions

Different Technical Approaches against botnets



1. Approach: Passive Honeypot

What happens?

- A provider's trap machine has been attacked by an infected customer machine.
- Data collection – IP-Address, time stamp, port number, type of the attack.

Legal issues?

- Data privacy (+)
 - Permission by § 28 para. 1 no. 2 BDSG
- Secrecy of Telecommunications (-)
 - The Provider is a party of the telecommunication and not a service supplier

2. Approach: Active Honeypot

What happens?

- The honeypot system of the provider access the infected customer machine.
- Data collection: the data from the passive approach + DNS-name, IP-Address of the download server, malware code and authentication information about the C&C server.

Legal issues?

- § 202a StGB – **Data Espionage!**
 - Provider is not authorized.
- Secrecy of Telecommunications (-)
 - The Provider is a party of the telecommunication and not a service supplier

3. Approach: SPAM-Trap

What happens?

- A dedicated email account (SPAM-Trap) collects SPAM emails.
- Data collection: sender email address, IP-Address, email header.

Legal issues?

- Data privacy (+)
 - Permission by § 28 para. 1 no. 2 BDSG
- Secrecy of telecommunications (-)
 - The Provider is a party of the telecommunication and not a service supplier.

4. Approach: DNS-Analyses

What happens?

- The name of the DNS of the C&C server is known. Contaminated machines can be identified by controlling the DNS access to the C&C-Server.
- Data collection: IP-Address, time stamp.

Legal issues?

- Secrecy of telecommunications (+)
 - Permission by § 100 para 3 TKG.
 - No general preventive analysis (name of the DNS is known)
 - Required for identifying of contaminated machines.
 - Used for stopping the unlawful use of the network
 - Reasonableness of means

5. Approach: Identification of botnets using Intrusion Detection Systems (IDS)

What happens?

- The IDS analyses the whole traffic using, which are typical for botnets.
- Data collection: the whole traffic, including the protocol and user data (email traffic, chat, websites requests etc.)

Legal issues?

- Secrecy of telecommunications (+)
 - Permission by § 100 TKG is problematic, if there are not pre-identified and concrete suspicion criteria at the port level
 - The provider should keep the deepness of traffic analysis in proportion to the technical needs for detecting of contaminated machines.
- Relevant to the criminal law - § 206 StGB Violation of Secrecy of telecommunications

6. Approach: Blocking or reducing the Internet access of the contaminated machine

What happens?

- The access to the internet of contaminated machines can be blocked or reduced .
- Data collection: no further data

Legal issues?

- Violation of the contract ???
 - (-) provided there are specific regulations in the Terms and Conditions;
 - Otherwise permission by § 314 BGB possible (Termination, for a compelling reason);
 - Important: notice period with the right to cure.
 - Problematic: the blocking of VoIP-Services.

7. Approach: Providing of data to other providers


What happens?


- Provision of data about contaminated machines to the providers of the involved networks.
- Data collection: IP-Address, time stamp, type of attack

Legal issues?

- Data privacy (+)
 - Permission by § 28 Abs. 2 Nr. 2a BDSG.
 - safeguard justified interests of the other provider as a third party
 - The other provider has a justified interest in detecting, locating and eliminating the unlawful use of his network.
- Important: the uncommitted use of the disclosed data is not allowed; the submitting provider should allude to.

Summary of the Approaches

- 
- Honeypot – passive approach
 - SPAM-Trap
 - Disclosure of information to the providers of the involved networks

- 
- Blocking or reducing the access to the Internet of the contaminated machines
 - DNS-Analysis

- 
- Intrusion Detection Systems
 - Honeypot – active approach

Trans-border Data Flow

Basic Requirements

Permission for
data handling
according to the
national law

Restrictions for ISPs :
Transmission for the
prevention of abuse

equivalent data
protection legal
framework in the
recipient state

Trans-border Data Flow

Equivalent data protection level ?

**Yes
Where?**

- Within the EU.
- Argentina,
Switzerland, Canada
(Decision of the EU-
Comission)

**No (third-country)
However allowed?**

USA Companies
participating in the
„Safe-Harbor-
Arrangement“
Problem: few ISPs

*Permission of the Data
Protection Authority
because of
conclusion or
performance of a
contract in the interest
of the data subject
between the controller
and a third party*

DRAFTED BUT NOT IMPLEMENTED:

- ◆ **Amendment 181, amending the E-Privacy Directive 2002/58/EC**
 - traffic data may be processed for the legitimate interest of the data controller for the purpose of implementing technical measures to ensure the **network and information security**, as defined by Article 4 (c) of Regulation (EC) 460/2004
 - Such processing must be restricted to that which is strictly necessary for the purposes of such security activity.

What are the rules in place at EU level?

- ◆ **Council Framework Decision (2005/222/JHA) from 24 February 2005 under the former so-called "third pillar"**
- ◆ **Addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service attacks**
- ◆ **For a transitional period until 2014, the Commission cannot take legal action to make sure Member States enforce these rules.**

NEW: Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA

- ◆ **The proposed Directive retains the current provisions of the Framework Decision:**
 - penalisation of illegal access,
 - illegal system interference and
 - illegal data interference

NEW: Proposal for a Directive on attacks against information systems, repealing Framework Decision 2005/222/JHA

◆ New elements:

- Penalisation of the use of tools (such as malicious software – e.g. 'botnets' – or unrightfully obtained computer passwords) for committing the offences;
- Introduction of 'illegal interception' of information systems as a criminal offence;
- Improvement of European criminal justice/police cooperation by
- strengthening the existing structure of 24/7 contact points, including an obligation to answer within 8 hours to urgent request and;
- Including the obligation to collect basic statistical data on cybercrimes

Thank you !

Ivo Ivanov
Attorney at law
General Corporate Counsel

ivo.ivanov@eco.de

t: +49 221 70 00 48 – 0

m: + 49 179 59 20 284

<http://www.eco.de>