

CoE Convention on Cybercrime and its transposition into German criminal law

Dennis Jussi

cand. iur. at Leibniz Universität Hannover

CoE Convention on Cybercrime

- Signed in Budapest, 2001 by (among 43 signees) all EU member states, Japan and the U.S.; as yet ratified by 21 states.
- Requires states to criminalise:
 - » illegal access to, and interception and interference of data
 - » misuse of devices (in relation to the prior)
 - » computer-related forgery and fraud
 - » violations of intellectual property rights
 - » computer-related child porn and racism
- Requires states to introduce investigative procedures:
 - » collection of traffic data; interception of content data
 - » international co-operation

Transposition into German criminal law

- 41. StrÄndG
(41st amendment to the criminal code [StGB])
- in effect as of 11 August, 2007
- 41. StrÄndG transposes substantive criminal law
- criminal proceedings will be transposed in conjunction with the transposition of the EC Data Retention Directive

Article 2: Illegal Access

- *“Each Party shall [...] establish as criminal offences [...], when committed intentionally, the access to the whole or any part of a computer system without right.
A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”*

Transposition: § 202a StGB

- a criminal offence is
 - » access to data
 - » by infringing security measures
- prior version
 - » obtaining data
- “without right”?
 - » general justification rules of German criminal law
 - » authorisation by the owner
 - owner of data content?
 - owner of storage device?
 - § 202a is part of chapter 15: offences against privacy
 - § 202a protects formal ownership
 - prosecution requires complaint by the victim (§ 205 StGB)

Article 3: Illegal Interception

- *Each Party shall [...] establish as criminal offences [...], when committed intentionally, the **interception without right**, made by technical means, of **non-public transmissions** of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.*
*A Party may require that the offence be committed with **dishonest intent**, or in relation to a computer system that is connected to another computer system.*

Transposition: § 202b StGB

- subsidiary to § 201 StGB (interception of phone calls, including VoIP) and §§ 148, 89 TKG (interception of radio transmissions, including WLAN)
- no requirement for “dishonest intent”
- “without right”?
 - » general justification rules of German criminal law
 - » authorisation by the owner
 - owner of data content?
 - owner of transmission devices?
 - § 202b is part of chapter 15: offences against privacy
 - § 202b protects formal ownership: communication participants
 - Who “owns” an IP packet?
 - prosecution requires complaint by the victim (§ 205 StGB)

Article 4: Data Interference

1. *Each Party shall [...] establish as criminal offences [...], when committed intentionally, the **damaging, deletion, deterioration, alteration or suppression** of computer data without right.*
2. *A Party may reserve the right to require that the conduct described in paragraph 1 result in **serious harm**.*

Transposition: § 303a StGB

- § 303a StGB has as such not been altered by 41. StrÄndG (apart from the criminalisation of preparation)
- “without right”?
 - » general justification rules of German criminal law
 - » authorisation by the owner
 - owner of data content?
 - owner of storage devices?
 - § 303a is part of chapter 27: damage to property
 - § 303a protects ownership of data; indications:
 - ownership of storage device
 - (technical) initiative to store data
 - (economic) value of data is an asset

Article 5: System Interference

- *Each Party shall [...] establish as criminal offences [...], when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

Transposition: § 303b StGB

- sabotage on data processing
- prior version: only business and administrative data processing; new: also private data processing
- new alternative: input of data
- “without right”?
 - » general justification rules of German criminal law
 - » authorisation by the person in control of data processing

Article 6: Misuse of Devices

1. *Each Party shall [...] establish as criminal offences [...], when committed intentionally and without right:*
 - a. *the production, sale, procurement for use, import, distribution or otherwise making available of:*
 - i. *a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*
 - ii. *a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,*
 - with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and*
 - b. *the possession of an item referred to [...].*
2. *This article shall not be interpreted as imposing criminal liability where the [facts] of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.*
3. *Each Party may reserve the right not to apply paragraph 1 [...].*

Transposition: § 202c StGB

- possession is not an offence
- computer program?
- designed for criminal offences? (dual use tools?)
- “without right”?
 - » preparation of a crime is abstract; there is not (necessarily) an intended victim that could authorise the production [etc.]
 - » no justification, but:
- intention of committing a crime (§§ 202a, 202b, 303a, 303b)

Handling of Hacker Tools

- Use tools that are not designed primarily for committing crimes.
- Have a clear authorisation for the offences that Art. 6 / § 202c refer to (namely Artt. 2-5 / §§ 202a, 202b, 303a, 303b).
- Do only share hacker tools with reliable partners (preferably with NDA) - not with the public.
- Limit access to hacker tools to the necessary.
- Journalise production / procurement of hacker tools and the intended use, and the actual use.

Thank You!



<http://creativecommons.org/licenses/by-nd/3.0/>