UDK 351.817:343.1
https://doi.org/10.18485/fb_ic4hs.2018.7

INTERCEPTION OF ENCRYPTED TELECOMMUNICATION AND THE SO-CALLED ONLINE SEARCH OF IT SYSTEMS FOR THE PURPOSE OF CRIMINAL PROSECUTION

Jan Dirk ROGGENKAMP*

Abstract: In 2008, Germany's Federal Constitutional Court ("FCC") rejected North Rhine-Westphalia's Constitutional Protection Act, which allowed the so-called online search of computers and other IT systems and the interception of encrypted telecommunication at the source[1]. The FCC stated that the society has a legitimate interest in the confidentiality and integrity of the IT systems protected by the constitution. In their view, the general right of personality encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems. However, with regard to preventive measures, the FCC deemed the measures acceptable within strictly defined limits. The secret infiltration of an information technology system by means of which the use of the system can be monitored and its storage media can be read is – according to the FCC – constitutionally only permissible if factual indications exist of a concrete danger to a predominantly important legal interest[2]. Whether or not the disputed measures may be permissible for the purpose of criminal prosecution, has been discussed ever since. In August 2017, an amendment to the German Code of Criminal Procedure was adopted. This allows the law enforcement authorities to secretly monitor encrypted telecommunications and to conduct so-called online searches of information technology systems (e.g. personal computers, smartphones, etc.). This extension of state powers raises strong constitutional concerns both with regard to human dignity and the so-called right to integrity and confidentiality of information technology systems. In addition to that, the new measures pose a threat to national (and international) IT security.

Keywords: online search, lawful interception, interception of encrypted telecommunication, criminal prosecution

---

* Professor, PhD, Berlin School of Economics and Law, jan.roggenkamp@hwr-berlin.de

[1] Also called ″source telecommunication surveillance″ as opposed to general telecommunications surveillance, because it allows to access data at the source prior to encryption via a special software which has to be secretly installed on the target computer or smartphone.

[2] Predominantly important are the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence.

1. BASELINE INFORMATION

In Germany it has been discussed for several years whether or not, and if so, and under which preconditions law enforcement agencies should be able to conduct a so-called online search of information technology systems and / or conduct a so-called source telecommunications surveillance (Jahn and Kudlich, 2007; Roggenkamp and Braun, 2011; Roggan, 2017). Both measures are to accommodate the difficulties in criminal investigations emerging if the targeted individuals use information technology, especially encryption techniques.

1.1. "ONLINE SEARCH"

In order to secretly (!) retrieve information stored on an information technology system (e.g. a computer, a smartphone, a tablet - hereafter "**Information Technology System**" or "**Target System**") the investigating law enforcement agency has to gain access to the system without the user (the target) noticing (Buermeyer, 2007:160). This is usually done by infiltrating into the Target System by taking advantage of its security loopholes (also called software vulnerabilities) and installing a spy program (so-called *"***Trojan Software***"*) (Buermeyer 2007: 163; Soiné, 2018:501; Pohlmann and Riedel, 2018:37). Using such Trojan Software makes it possible to monitor the use of the Target System, in order to view the data on the storage media and extract it, and/or to control the Information Technology System remotely (Freiling, Safferling and Rückert, 2018:16). This measure is called *"Online-Durchsuchung"* in Germany, which literally translates as "**Online Search**" (and is not to be confused with a mere search for information on the Internet via search engines and the like).

1.2. SOURCE TELECOMMUNICATION SURVEILLANCE

The so-called source telecommunication surveillance ("**STS**") is a special method of telecommunications surveillance, which is used to access and extract telecommunications data (e.g. speech, messages) at the source of communication (e.g. a smartphone or laptop). It is thus deemed necessary to intercept potentially encrypted telecommunication e.g. via messenger apps such as WhatsApp or Telegram before it is being encrypted, or after it has been decrypted (Roggenkamp and Braun, 2011:681). As with Online Searches, it is necessary to infiltrate into the Target System and implement Trojan Software that (clandestinely) extracts the relevant telecommunications data and submits it to the law enforcement agency (Buermeyer and Bäcker, 2009:434).

1.3. THE "ONLINE SEARCH JUDGEMENT" BY THE GERMAN FEDERAL CONSTITUTIONAL COURT

In 2008, Germany's Federal Constitutional Court (*"***FCC***"*) rejected North Rhine-Westphalia's Constitutional Protection Act (North Rhine-Westphalia Constitutional Protection Act, 2006), which empowered the constitution protection authority of the federal state of North Rhine-Westphalia to conduct Online Searches and STS for preventive purposes (FCC 2008).

The FCC stated that the society has a legitimate interest in the confidentiality and integrity of the Information Technology Systems protected by the German constitution (i.e. the *Grundgesetz* – "**German Basic Law**"). In their view the general right of personality encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems (FCC 2008: Headnote 1).

However, the FCC deemed such measures, if conducted with a preventive objective, acceptable within strictly defined limits. The secret infiltration of an Information Technology System by means of which the use of the system can be monitored and its storage media can be read is – according to the FCC – constitutionally (only) permissible if factual indications exist of a concrete danger to a *"predominantly important legal interest*". Predominantly important legal interests are defined as *"the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence"*.

Furthermore, the FCC held that insofar as empowerment of the investigating authority is restricted to a state measure by means of which the contents and circumstances of on-going telecommunication are collected in the computer network, or the data related thereto is evaluated, the encroachment is to be measured against the right to privacy of telecommunications (German Basic Law: Article 10.1) alone.

1.4. PERMISSIBILITY FOR PURPOSE OF CRIMINAL PROSECUTION

Whether or not these measures may be permissible for the purpose of criminal prosecution has been discussed ever since. In August 2017, an amendment of the German Criminal Code of Procedure (*"***CCP***"*) entered into force expanding the powers of law enforcement agencies to conduct Online Searches and intercept encrypted telecommunication via STS. In August 2018, a constitutional complaint against the aforementioned amendment has been filed with the FCC deeming it unconstitutional (Martin, 2018).[3]

2. INFRINGEMENT OF HUMAN DIGNITY?

2.1. INTRUSION OF PRIVACY

Both measures, Online Searches and STS, enable law enforcement agencies to secretly intrude into the privacy of a person and collect all-encompassing intimate information about this person. The amount of private information, which may be gathered, is unparalleled in comparison to other measures such as house searches (Roggan, 2017).

Smartphones in particular, but also other Information Technology Systems, have become constant and personal companions to their users (Proner, 2015). They "know" every location the user visits or has visited, they *"*know*"* the users likes and dislikes. Information Technology Systems are used to share and discuss political, religious or social topics – sometimes highly personal. Users "confer" with search engines before a new car is bought, but also in case of illness or relationship problems. The search for a life partner is assisted by so-called apps, as is the search for the current cinema or theatre programme. Holiday

[3] Disclosure: the author of this article is one of the legal representatives of the plaintiffs.

pictures, pictures of kids or erotic "selfies" are shared via messenger services. If a smartphone, which is connected to the Internet, is being surveilled, it is actually a surveillance of the inner world of ideas, emotions and common behaviour (Roggan, 2017:817). It is possible to generate a personality profile, which could not be more detailed.

2.2. HUMAN DIGNITY

The inviolable fundamental right to human dignity is not only the foundation of the right to privacy (Floridi, 2016:307), but directly protects the so-called core area of private life of every human being (pro omnibus Papier, 2017:3028).

According to the FCC, secret surveillance measures carried out by state agencies must absolutely respect this inviolable area. Even overriding interests of the public cannot justify encroachment on it. The FCC states that the development of the personality in the core area of private life includes the possibility to express inner events such as perceptions and feelings, as well as considerations, views and experiences of a highly personal nature, without fear that state agencies may have access to them (FCC 2008: Para 271).

With regard to the aforementioned (B. 1.) use of smartphones etc., it is the view expressed here that the secret surveillance of a personal Information Technology System is a disrespect for the inviolable core area of private life and, thus, unconstitutional. The secret investigation of a person's world of thought that goes hand in hand with the measures discussed here is, in the view held here, an unjustifiable violation of human dignity.

3. INFRINGEMENT OF RIGHT TO CONFIDENTIALITY AND INTEGRITY OF INFORMATION TECHNOLOGY SYSTEMS?

However, the FCC held in 2008 that an Online Search is "only" to be seen as an encroachment on *"the general right of personality in its particular manifestation as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems"* (FCC, 2008: Para 166).

3.1. PREDOMINANTLY IMPORTANT LEGAL INTERESTS

The FCC stated that such an encroachment may (only) be provided for *"if the empowerment to encroach makes it contingent on the existence of factual indications of a concrete danger to a predominantly important legal interest"*.

With regard to measures, which serve the purpose of criminal prosecution, it is unclear if and how this requirement can be transposed. Criminal investigations and prosecutions do not aim at averting *"concrete dangers to predominantly important legal interest"* but serve mainly to enforce the State's right to inflict punishment if a crime has been committed. Whether this is a *"predominantly important legal interest"* in itself is to be doubted. A constructive approach asks whether the crime, which is investigated, is actually a realisation of a danger to the aforementioned *"predominantly important legal interest"* and if an Online Search may have been conducted in order to prevent the realisation, had the danger been known in time. Hence, the investigation of a murder or a hostage taking may be carried out via online search but not crimes such as corruption, theft, receiving and handling, drug dealing, etc.

The new regulation of the CCP from 2017 (see A. 4.) does not comply with these requirements. Online Searches are only to be permitted in cases where there is a "particularly serious crime". However, offences such as money laundering, commercial receiving of stolen goods or bribery are also considered to be "particularly serious" under the new provisions of the CCP (see Sect. 100b Para 2 CCP), which is too broad to meet the aforementioned requirements. Moreover, the new CCP merely requires that "certain facts give rise to suspicion" that the target person is the perpetrator or participant in a "particularly serious crime". In order to do justice to the seriousness of the encroachment, however, higher demands must be made than just a simple initial suspicion.

3.2. SUITABLE STATUTORY PRECAUTIONS

Furthermore, according to the FCC (FCC, 2008: Para 257), the empowerment to effect secret access to Information Technology Systems *"must be linked with suitable statutory precautions in order to secure the interests of the person concerned under procedural law. If a norm provides for secret investigation activities on the part of the state which – as here – affect particularly protected zones of privacy or demonstrate a particularly high intensity of encroachment, the weight of the encroachment on fundamental rights is to be accounted for by suitable procedural precautions".*

a. Reservation of judicial order

With regard to this, the FCC holds that secret access to an Information Technology System is in principle (the exception being imminent danger) to be placed under the reservation of a judicial order in order to protect the concerned individual from unlawful use of the measure.

The new CCP (Sect. 100e Para 2 CCP) fulfils this requirement by demanding not only a judicial order by a single judge, but by a chamber of the district court (*Landgericht*).

b. Protection of core area of private life

In addition to that, adequate statutory precautions to avoid encroachments on the absolutely protected core area of private life have to be provided (FCC, 2008, Para 270).

The FCC acknowledges, *"In the context of secret access to an information technology system, the danger exists that the state agency might collect personal data which is to be attributed to the core area. For instance, the person concerned may use the system to establish and store files with highly personal contents, such as diary-like records or private film or sound documents. Such files can enjoy absolute protection, as can for instance written embodiments of highly personal experiences [...]. Secondly, insofar as it is used for telecommunication purposes, the system can be used to transmit contents, which can equally fall within the core area. This applies not only to speech telephony, but for instance also to telecommunication using e-mails or other Internet communication services [...]. The absolutely protected data can be collected with different types of access, such as with the inspection of storage media, just as with the surveillance of on-going Internet communication or indeed with full surveillance of the use of the target system."* (FCC, 2008: Para 272)

However, although the FCC does not hold that such secret access to highly personal contents is a violation of human dignity in itself, it deems that it is necessary to provide statutory precautions to protect the core area of private life. These precautions have to be provided on two levels, these being (1) the collection of information and (2) the evaluation of information collected. The FCC holds that a statutory empowerment must ensure *"as far as possible"* that no data is collected which relates to the core area (FCC, 2008: Para 277).

At first glance at the new CCP, the legislator seems to fulfil this requirement by stating that the law enforcement agency conducting an Online Search has to apply technical means to ensure ″as far as possible″ that information relating to the core area of private life is not being collected (cf. Sect. 100e Para 3 CCP). A closer look shows, however, that the provision is inadequate as there are no technical means (at least not yet) to comply with this statutory ″precaution″. In order to avoid the collection of information, which is of a highly personal nature, the only viable approach is a ″risk evaluation″ with regard to the Target System. Such a risk evaluation is undertaken under German law in cases where a house or a flat is monitored acoustically (Sect. 100c CCP). In these cases the law enforcement agency has to – by law – evaluate whether it is to be expected that discussions/events in the particular room will be of a highly personal nature. If this is the case (e.g. bedroom of a couple), the monitoring of this room is not allowed (cf. Sect. 100e Para 4 CCP). A similar approach is – according to the view expressed here – possible (and necessary) with regard to Information Technology Systems. It has to be evaluated whether it is to be expected that the Target System will be used for highly personal purpose (e.g. personal smartphone). If this is the case, the law enforcement agency must refrain from conducting a (secret) Online Search.

3.3. PROTECTION OF DATA AND IT SECURITY

In order to guarantee sufficient protection for the integrity of the Target System, it is the view expressed here that it must be stipulated by law that the Trojan Software used is examined by at least one independent body (e.g. the Federal Data Protection Authority) for compatibility with data protection law before use. This is the only way to avoid third parties also having access to the mobile phones and laptops of the monitored users through unknown back doors or – in the worst case – a data breach (Roggenkamp, 2018:610).

In addition, it must be stipulated by law that the state may not exploit unknown security gaps (so-called zero day exploits) in order to install the software. In the view of the complainants of four constitutional complaints currently pending[4], this must be prohibited – as must the procurement and "storage" of such "exploits" – in order to guarantee national (and international) IT security (Pohlmann and Riedel 2018:37). Incidents such as the "WannaCry" infection of millions of computers all over the world, allegedly caused by an "exploit" lost by the NSA (Patrizio, 2017), must not be repeated.

With regard to both Online Searches and STS, the new regulation of the CCP is incompatible with data and IT security.

---

[4] Only one of the complaints has been published so far: https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf.

4. CONCLUSION

According to the view expressed here, it is preferable to regard online searches and STS as unconstitutional and unjustifiable encroachments on human dignity and to refrain from corresponding measures. If one sees this differently, as does the FCC, then, however, sophisticated legal precautions must be taken to protect the personal rights of the persons concerned and general IT security. The regulations in the new German CCP do not meet these requirements.[5]

5. BIBLIOGRAPHY

Buermeyer, U. (2007). Die "Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme [The "online search". Technical background of covert sovereign access to computer systems]. *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* [Online journal for highest court rulings on criminal law] (HRRS), [online] 2007(4), pp.154 - 166. Available at: https://www.hrr-strafrecht.de/ .

Buermeyer, U. and Bäcker, M. (2009). Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO [On the illegality of source telecommunications surveillance on the basis of Sect. 100a CCP]. *Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht* [Online journal for highest court rulings on criminal law](HRRS), [online] 2009(10), pp. 433 - 441. Available at: https://www.hrr-strafrecht.de/.

Federal Constitutional Court of Germany (2008). Judgment of the First Senate of 27 February 2008 - Ref. 1 BvR 370/07. Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology*, 29(4), pp. 307 - 312.

Freiling, F., Safferling, C. and Rückert, C. (2018). Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen [Source telecommunication surveillance and online search as new measures for law enforcement: Legal and technical challenges]. *Juristische Rundschau* [Legal review] (JR), 2018(1), pp. 9 - 23.

Gesetz über den Verfassungsschutz in Nordrhein-Westfalen [North Rhine-Westphalia Constitution Protection Act (2006)] in the version of the Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen [Act Amending the Act on the Protection of the Constitution in North Rhine-Westphalia] of 20.12.2006. *Law and Ordinance Gazette of North Rhine-Westphalia* (GVBl NW) 2006, p. 620).

Grundgesetz für die Bundesrepublik Deutschland (GG) [Basic Law for the Federal Republic of Germany (1949) - (German Basic Law)], 23.5.1949, with subsequent

[5] Four constitutional complaints were lodged with the FCC against the new regulation. However, a decision is not expected for a few years.

amendments. Available at https://www.gesetze-im-internet.de/englisch_gg/index.html.

Jahn, M. and Kudlich, H. (2007). Die strafprozessuale Zulässigkeit der Online-Durchsuchung [The admissibility of online searches in criminal procedural law]. *Juristische Rundschau* [Legal review] (JR), 2007(2), pp. 57-61.

Martin, D. (2018). Germany's government hackers face Constitutional Court. *Deutsche Welle News* (07.08.2018). Available at https://www.dw.com/en/germanys-government-hackers-face-constitutional-court/a-44988326.

Papier, H. (2017). Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft [Rule of law and protection of fundamental rights in the digital society]. *Neue Juristische Wochenschrift* [New Legal Weekly] (NJW), *70*, 42, 3025 - 3031.

Patrizio, A. (2017). Microsoft to NSA: WannaCry is your fault. [online] *Network World*. Available at: https://www.networkworld.com/article/3196222/security/microsoft-to-nsa-wannacry-is-your-fault.html.

Pohlmann, N. and Riedel, R. (2018). Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen [Criminal prosecution must not compromise IT security. on the Internet]. *Datenschutz und Datensicherheit* [Data Protection and Data Security] (DuD), 42(1), pp.37 - 44.

Proner, P. (2015). The Extended Self – Die Bedeutung von Smartphones für Nutzer und Konsumenten [The Importance of Smartphones for Users and Consumers]. [online] *Think with Google*. Available at: https://www.thinkwithgoogle.com/intl/de-de/insights/kundeneinblicke/the-extended-self-die-bedeutung-von-smartphones-fur-nutzer-und-konsumenten/.

Roggan, F. (2017). Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit [The criminal procedural source telecommunication surveillance and online search: Electronic surveillance measures with risks for accused persons and the general public]. *Strafverteidiger* [Defence Counsel] (StV), 37(12), p. 821.

Roggenkamp, J. and Braun, F. (2011). Ozapftis - (Un)Zulässigkeit von "Staatstrojanern" [Ozapftis - (In)permissibility of "State Trojans"] *Kommunikation und Recht* [Communcation and Law] (K&R), 2011(11), pp.681-686.

Roggenkamp, J. (2018). *Handbuch europäisches und deutsches Datenschutzrecht* - § 21 - Datenschutz und präventive Tätigkeit der Polizei [European and German data protection law handbook - § 21 - Data protection and preventive police work]. Munich: C.H. Beck / Specht, L. and Mantz, R. (Editors), pp.599 - 622.

Soiné, M. (2018). Die strafprozessuale Online-Durchsuchung [The criminal procedural online-search]. *Neue Zeitschrift für Strafrecht* [New Journal for Criminal Law] (NStZ), 38(9), pp.497 - 504.

Strafprozessordnung (StPO) [Criminal Code of Procedure - (CCP)], 1.2.1877 in the version published on 7 April 1987. *Bundesgesetzblatt* [Federal Law Gazette] Part I p. 1074, 1319), with subsequent amendments. Available at: https://www.gesetze-im-internet.de/stpo/.