Locating criminal investigative measures in a virtual environment

Where do searches take place in cyberspace?

C. CONINGS*

Introduction

The territoriality principle limits state sovereignty and its accompanying competencies to a national territory. Likewise, a government's authority to investigate criminal acts is restricted to the territory falling under the competencies of such government. If a government wants to perform investigative acts abroad, it must rely on an official request for legal assistance if no international agreement for cooperation applies. Due to the digitisation of criminal evidence and the worldwide mobility of data, the need for international cooperation seems to expand enormously. Therefore, states are looking into possibilities to strengthen and speed up international cooperation. However, the underlying and more fundamental question on the establishment of procedural jurisdiction has more or less been neglected. The first thing we need to know is when a state is acting in it's own territory, and thus within its competence, and when it is investigating in the territory of another state, for which it would need international cooperation. Whilst speeding up international cooperation is definitely imperative, we first have to find out in which circumstances such cooperation is needed. In the light thereof, this proposal is aimed at defining the relevant "here" and "there"[1] in order to establish procedural jurisdiction in a digitising world.

The following text is the summary of a legal research done in the framework of the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCentre). The full text of the research is available online.[2] The concrete proposal can be found on p. 10 et seq. of this text. A schematic overview can be found on p. 15 and 16 of this text.

I. Determining location in Criminal Procedure Law

1. TRADITIONAL OBJECT-ORIENTED APPROACH – Nowadays, It is often difficult to establish the place where a government exercises its investigatory powers. Few problems regarding procedural competencies arose in the past. Traditionally, physical evidence is collected where the evidence is to be found. The traditional way of locating criminal investigative measures is therefore object-oriented. The object of the search, namely the sought evidence, determines the location of the search.

2. WIRETAP: SUBJECT-ORIENTED APPROACH - Wiretap competences constituted a first challenge in this matter. According to the traditional territoriality approach, the interception should be located where the evidence (the conversation) is intercepted. However, the European Union puts forward another localisation criterion for wiretap activities, namely the location of the person whose

---

* The author is a PhD candidate at the Institute for Criminal Law of the University of Leuven and affiliated researcher at the B-CCENTRE. This contribution has been published in Dutch in *Nullum Crimen* 2014, no. 1, 1-25.

[1] Cf. J. DASKAL, "The UN-Territoriality of Data", *Yale L.J.* 2015, vol. 125, 326-398 (focusing on the American approach).

[2] https://www.b-ccentre.be/wp-content/uploads/2015/02/B-CCENTRE-Research-Report-Legal_FINAL.pdf , 43-72.

communication is being intercepted.[3] The focus thereby shifts from the object sought, i.e. the evidence (*object-oriented approach*) to the subject under investigation, i.e. the investigated person (*subject-oriented approach*). The wiretap takes place at the location of the subject under investigation. The fact that the communicating partner is possibly abroad does not hamper the unilateral competence of the state on whose territory the investigated subject is located, to intercept the communication.

3. DIGITIZED EVIDENCE: LINK WITH DIFFERENT PHYSICAL LOCATIONS - Whilst wiretap was a first, smaller challenge, digitisation of evidence questions the basic understanding of the location of investigative acts substantially. Compared to traditional telephone conversations, digital evidence is linked to national territories in many different ways. In contrast to traditional telephone communication, digitised conversations and acts (such as emails send by means of webmail applications, remarks and discussions on social media and images and documents stored in the cloud) often leave traces that are stored with a third person (mostly an Internet service provider). Consequently, information about a person is no longer only to be found in paper files, boxes or hard disks in a person's home or office but also, and increasingly, on servers and computers of these third parties. Furthermore, such third persons can manage their servers at a distance. This entails that the location of the service provider and the place where the data are stored may differ. For example, Facebook is an American service provider, but it can store its data on servers that are located anywhere in the world. To make matters even more difficult, when information is sent to, or requested from, a server, it randomly travels between the user and the storage place. This means the data can also be located at technical intermediate stops (e.g. an Internet Exchange Point (IXP)), albeit only for a limited period of time. The Internet reality separates the *location of the data* (which can be searched within the scope of a criminal investigation) from the *location of the persons* (whose fundamental rights may be affected by such investigation) in a way never before encountered. The location where data are stored, the location of the consulted service and the location where those data and such service can be used may differ. Furthermore, copies of data can be stored at several places at a time (cf. *cloud computing*)[4] and the location of data can easily change. Last but not least, the investigating law enforcement agencies are not necessarily on the territory where the sought information is to be found, neither are they necessarily to be found on the territory where the investigated person or consulted service provider is to be found. As is the case with the users, the law enforcement agencies are location independent.[5]

4. A NEW PROCEDURAL LOCATING ISSUE - Consequently, when law enforcement agencies collect evidence in the "virtual world" (e.g. through looking at a Facebook account, Google calendar, Dropbox account or a YaHoo! webmail account), one of the questions that arises, pertains to the location of their investigative actions. In such a case, is the investigative act located in the territory where the sought data are stored, or is it located in the territory where the investigated person can be

---

[3] Articles 18-20 of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, www.eclan.eu (Referred to hereafter as the EU Convention on Mutual Assistance in Criminal Matters.); Explanatory report to the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Official Journal* C 379 of 29 December 2000, no. 379, 20-21. The explanatory report explicitly mentions that a state's interception of communication to or from its territory implies a measure on its own territory. The regulatory framework on the European Investigation Order does not change this approach. Art. 30 and 31 Directive 2014/41/EU of the European Parliament and the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, *Pb.L.* 1 May 2014, nr. 130. The directive has to be transposed by 22 May 2017 in all Member States.

[4] J. DASKAL, "The UN-Territoriality of Data", *Yale L.J.* 2015, vol. 125, (326) 368.

[5] M. HILDEBRANDT, "Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal*, 2013, afl. 63, 220-221.

found? Is the investigating authority operating in the territory from where they perform the investigative act? Does the location of the service provider play a role in this matter? Each criterion represents a different link between the digital evidence sought and the physical reality. Consequently, each criterion can locate the investigative act on a certain territory. However, the question is: which criterion must be the decisive one?

II. Locating investigative acts in cyberspace

5. TYPES OF SEARCHES – We have to distinguish between two types of searches for digital evidence. The first involves law enforcement agencies keeping a "virtual eye" on a person in real time (hereafter: *virtual search in real time*), whilst the second involves a search for stored data, independent of a simultaneous action by the investigated subject (hereafter: *search for stored data*). Virtual search in real time refers to observing virtual actions of the investigated subject such as opening websites, communications or files while those actions are taking place.[6] Using key loggers[7], which register keystrokes and mouse movements, is another example of virtual search in real time, as is viewing or listening to communications at the moment at which it is being conducted by the investigated subject (e.g. Skype or chat conversation, typing and sending emails). In contrast, the search for stored data is independent of the investigated subject's simultaneous actions regarding the data being investigated. This concerns an open or covert search within profiles on social media or accounts providing access to cloud services (e.g. Dropbox or iCloud) or webmail services (e.g. Yahoo!, Hotmail or Gmail).

1. Virtual search in real time

6. CURRENT CONTRADICTORY APPROACH - The current approach of the location of virtual searches in real time are contradictory. Both the EU Convention on Mutual Assistance in Criminal Matters and the Convention on Cybercrime apply the subject-oriented approach by referring to the location of the communicating party under investigation. However, without additional explanation, the Convention on Cybercrime seems to require that competence should also be conferred to the state where the computer system or the telecommunication equipment transmitting the communication is located. In this way, the Convention combines the subject- and object-oriented approaches to locating real-time investigative acts. When a state intercepts communication at an intermediate station on its territory that is only used for transmitting communication, then, according to the Convention on Cybercrime, such interception occurs on the territory of the intercepting state, which can intercept the communication unilaterally. The fact that the communicating parties are located somewhere else is irrelevant. This is in sharp contrast to the view in the European Union. Article 20 of the Convention on Mutual Assistance in Criminal Matters provides for the possibility of intercepting communication of persons who are abroad without requiring mutual legal assistance. Although no judicial *assistance* is required, the Article *does* actually require notification to and consent from the state where the person whose communication is to be intercepted is located.[8] With a view to legal certainty, it is

[6] This can technically be done by using spyware, for example.
[7] We do not deal with the question whether investigative institutions are allowed to use key loggers. We only consider the question concerning the location of investigative actions.
[8] If it is known that the person is located on the territory of another Member State before the interception order is given, such notification must be sent before the interception takes place. In other cases, the notification must be made immediately after it has become known that the person is located on the territory of the Member State to be notified. Compare: article 31 Directive European Investigation Order.

recommended that the location method of the Council of Europe and the location method of the European Union be harmonized.

7. TOWARDS A UNIFORM LOCATING PRINCIPLES: FOCUS ON SUBJECT – Both the Convention on Cybercrime and the EU Convention on Mutual Assistance in Criminal Matters apply a subject-oriented principle: the state on whose territory the subject is located is territorially competent to perform investigative measures in real time in regard to the said subject. This seems logical from the perspective of the principle of sovereignty. The sovereign authority of the state where the subject is located (hereafter: subject state) includes the competence of controlling actions performed on and communications conducted from or to its territory. This is subject to the conditions outlined in its national law and the rights and freedoms to which it has committed itself at an international level. Moreover, a completely subject-oriented approach clearly delineates a territorial border with regard to sovereign competence. When the subject crosses the border, the possibility to unilaterally continue the real-time search also lapses. As a matter of fact, international cooperation is required every time the subject to be intercepted is located abroad, even if no foreign technical assistance is needed. This approach provides sufficient legal certainty. Legal protection, in particular protection of the right to privacy[9], is provided in accordance with the law of the country in which the legal subject is located, and from where he performs actions and communicates. The state where the subject is located is entitled to exclude other states and can in this way offer its subjects protection against any foreign interference with their fundamental rights that is unlawful according to national law.

8. SUPPLEMENT[10] OF OBJECT REJECTED – We are of the opinion that it is not advisable to supplement the subject-oriented authority with an object-oriented authority, whereby the location of the data is per se decisive. In the Convention on Cybercrime, we find a criterion that is based solely on the technical presence of the data. According to this approach, the moment data are technically present on a state's territory, that state can investigate the data in real time in accordance with its national regulations. We are however of the opinion that this technical criterion is not appropriate. The investigative method could in fact be used to deliberately search for data relating to communications conducted between persons who are abroad, without any form of international cooperation and without there being a demonstrable link between the data investigated and the investigating state (e.g. by monitoring an Internet Exchange Point[11]). After all, the IT systems (routers) through which the data pass are, to a certain extent, determined randomly.[12] Even if both communicating parties and the communication service provider are located on the territory of one state, it is possible that other states can access the communication under their national regulations, merely because of the technical construction and operation of the Internet. In this approach, the territoriality plays a limited role. As a result, each state loses control of the protection of persons who

---

[9] Art. 8 ECHR.

[10] An exclusive object-oriented approach would be possibile as well. However, we do not look into this possibility here. Reasons why such an approach is not desirable are comparable to those elaborated in the part concerning virtual remote searches. (see below, no. 14 and 15.)

[11] i.e. a type of internet hub to which various service providers' networks are connected and through which they mutually exchange their communication. With regard to the possibility of monitoring an Internet Exchange Point, see: F. BHATTI, J. SOUTER, "ExSERT: Enabling Distributed Monitoring at Internet Exchange Points", 2005, http://saleem.host.cs.st-andrews.ac.uk/publications/2005/lcs2005/lcs2005-hbs2005.pdf; see as well: G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, *kms2.isn.ethz.ch*, 21-23.

[12] J. GULDENTOPS, *Geschiedenis en het internet: een historische, methodologische en heuristische benadering van de informatiesnelweg*, Leuven, Acco, 1996, 9; G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, *kms2.isn.ethz.ch, 4;* See as well: Verslag namens de commissie, *Parl. St.* Senaat 1999-2000, no. 2-392/3, 22.

are located on its territory and who perform actions there or communicate from there, against infringements of their fundamental rights by foreign state agents, solely because of the technical construction of the internet. In this way, there is no longer any legal certainty for the legal subjects. We are therefore of the opinion that if a country wishes to intercept data that are by chance present on its territory at a certain moment, state sovereignty and mutual respect between states require more precise rules regarding international cooperation.[13]

2. The search for stored data

9. CURRENT OBJECT-ORIENTED APPROACH – According to the traditional object-oriented approach, we could state that the remote search for digital evidence[14], which is stored on an IT system abroad, can only be obtained by means of international cooperation. This point of view is not only to be found in doctrine.[15] The Council of Europe and the Belgian national legislator seem to use this as point of departure as well. The criterion of the location of the sought after data appears to be impractical though. Investigating authorities are increasingly confronted with the fact that the sought after data are stored abroad, which puts them in a disproportional need for international cooperation. The international cooperation is usually characterized by delays, which implies a huge risk of loss of evidence. Lack of time is however not the only problem impairing the efficiency of the current system. Lack of knowledge is another serious stumbling block (cf. loss of object location). It often appears to be difficult or impossible to pinpoint the precise location of data (cf. cloud computing). Besides, the location of data can easily and quickly change. In order to make a criterion for procedural jurisdiction practicable, it is extremely important that investigating authorities can easily estimate in advance how they can apply it in the case they are working on.[16] The criterion may also not be subjected to too much change. That is why the location of data does not seem to be a good criterion. Furthermore, applying the traditional object-oriented approach to searches for digital proof is not at all self-evident. There is an important difference between traditional searches for evidence and searches for digital proof. In the latter case, the place where the evidence is to be found and the place(s) of access to the evidence no longer necessarily coincide. A person can store data across borders but access them and use them where and when he pleases. Consequently, a new situation has arisen, which is not at all comparable to the searches for physical proof in the real world. For this reason, we consider a few other possibilities to locate remote searches for stored data and compare the current object-oriented point of view with the most suitable alternatives.

---

[13] By way of comparison: B. DE SMET, "Registratie en lokalisatie van telecommunicatie" in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE, *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer*, Mechelen, Kluwer, 2008, 29.

[14] E.g. the network search (the extension of the search in an IT system to an IT system connected to it, which is located at a distance) or the secret variant thereof, which we like to call the "online investigation". See C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 23-32. In more practical terms, one can think of searching a Dropbox account, an account on social media or a webmail account.

[15] See: N. SEITZ, "Transborder search: a new perspective in law enforcement?", *Yale Journal of Law and Technology* 2005, Vol. 7, 22 ff; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[16] J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

A. Alternative locating criteria

10. LOCATION OF INVESTIGATING AUTHORITIES REJECTED - The first possible criterion to locate the search for stored data is the location of the investigating authorities. According to this view, the place where the investigating official is physically located and where he reaches out to the data is also the place where the search takes place. However, we find this view too far-reaching. An extremely large amount of information, whether encrypted or not, is directly available through the internet. Such information may often relate to foreign matters, persons and objects. To choose the location of investigating authorities as a decisive criterion would therefore clearly cause an impairment of the sovereignty of other states because persons and occurrences on their territory could be cut off from their legal protection, merely and solely due to a presence in the virtual landscape. Moreover, this view impairs legal subordinates' legal certainty. In this case, they have no idea whatsoever as to when information regarding them, which can be accessed at a distance, can be viewed and controlled by foreign authorities.

11. LOCATION OF THE INVESTIGATED PERSON: REJECTED – A second possible approach is to locate the search for stored data in the same way as virtual searches in real time by focusing on the location of the investigated person. However, merely extending the application of the locating principle as it applies to real time searches is over-simplifying matters. Searches in real time look at the investigated person's comings and goings at the moment that the search is taking place. By locating such investigative acts in the place where the investigated person is to be found, states are able to control in real time the communication and actions conducted or performed on their territory. By contrast, using the location of the investigated person as a criterion to locate the remote search for stored data would imply the following: entering a territory for a holiday, business trip or stopover would make the virtual past of the concerned person, which is stored by means of all types of online accounts, searchable by the local authority purely in accordance with national regulations. According to this view, every time a person transcends the border he would necessarily always take all his digital belongings with him, so to speak, in so far as these are accessible from a distance. Leaving a virtual past at home would then no longer be an option. In our view, this would involve a grave impairment of the free movement of persons and their self-determination not to submit matters to the direct competence of a foreign authority. Having regard to the territorial delineation of sovereignty, an individual exposes himself to the legal competence of a foreign authority every time he transcends the border. His comings and goings fall under the control of the foreign authority, as do the objects he takes with him. If the person does not wish to subject objects, which may contain proof of communications or actions from the past (such as letters, documents, photographs, a laptop or smartphone), to such sovereign authority, he should not take them along when transcending the border but should leave them at home. We find that depriving persons of such a choice, purely because of the virtual accessibility thereof, displays a lack of subtlety and is undesirable.

12. LOCATION OF HABITUAL RESIDENCE – An investigated subject's habitual residence is another possible criterion to determine the location of the remote search for stored data. This approach locates a person's virtual living environment (i.e. all the digital data to which the respective person has remote legal access, such as online profiles on all types of websites, with the exception of profiles hacked by the respective person). It combines the focal point of someone's virtual life with that of his physical life. For example, when law enforcement agencies wish to access a suspect's Dropbox account, there would be no problem in terms of International Law if the suspect's habitual residence is located on the national territory of those law enforcement agencies. Moving one's habitual residence also entails moving one's virtual living environment. A person is assumed to leave his virtual past at home when

he physically transcends borders. Having regard to the locating principle in the case of searches in real time, the foreign authority can in fact unilaterally access the respective person's present-day virtual life, e.g. observing which data the respective person consults during his stay. Furthermore, the foreign authority can unilaterally access the data which the respective person actually takes with him across the border (e.g. data stored on the Smartphone that he carries with him). By contrast, access to the virtual past, independent from the investigated person's simultaneous use of data, such as an online search of a Hotmail or Dropbox account or a Google Calendar, is in principle only possible by means of cooperation with the country where the investigated person has his habitual residence (however, see no. 17 et seq., below). As in Tax Law, we could work with presumptions as to the habitual residence of the concerned person.[17] The habitual residence is then presumably the place where the respective person is registered with the national registry. That presumption is refutable, however. In the case of a married or legally cohabiting person, there is an irrefutable presumption that the habitual residence is the place where the family is settled.

13. LOCATION OF SERVICE PROVIDER CONSULTED – Finally, the investigative act could also be located by means of the location of the service provider through whose services the searched data are generated and/or stored. Under this approach, it is possible for the United States to examine data on Facebook, irrespective of where Facebook has stored the data and irrespective of the location or nationality of the person to whom such data belongs. This would in any event be more practical than the current criterion because investigation is no longer hindered by the loss of location of the data. Consequently, we also consider this criterion in deciding which main criterion must be taken into account to determine territorial procedural competence.

B. Comparison

14. STATE SOVEREIGNTY - During the preparatory works of the Convention on Cybercrime, it became apparent that it was not clear whether a direct search for data stored abroad constituted an infringement of the sovereignty of the state where the data are stored (hereafter: state of storage). The question whether a more subject-oriented power would therefore infringe the sovereignty of the state of storage remains unanswered. In contrast, the following question does not arise in the preparatory documents, although it is just as important: does the current object-oriented approach constitute an infringement of the sovereignty of the state where the investigated person is normally to be found (state of residence)? However, it seems to us that, in an object- or service-oriented approach, an infringement of the sovereignty of the state of residence is more likely to occur. According to the object-oriented approach, the states with the largest storage capacity assume sovereign power over data of persons regardless of where they are located in the world. The data constitute a form of externalisation of activities performed on the territory of another state. The place where a virtual life is actually lived is irrelevant in the object-oriented approach. The same applies when the search is to be located in the service provider's state. The state on whose territory the virtual actions are normally performed or the virtual communication is normally conducted (i.e. the state of residence) does not have any competence to autonomously control actions and communications on its territory, apart from real-time search. That state does not have an autonomous access competence to the data, whereas the respective legal subject can consult and use the data on his territory. In order to make control possible, the state of habitual residence would always have to cooperate with the state where the data are stored

[17] See art. 2§1, 1° Code of Income Revenue Taxes, *Belgian Official Gazette* 30 juli 1992.

or the state from which the service is provided. Moreover, the place where the data are stored is most certainly not always the same as the place where the consulted service provider is located. In that case, the object-oriented approach allocates the sovereign competence regarding the data to a state which shows very little connection with the investigated activity or person. In this way, the legal framework is completely alienated from the reality that it aims to regulate.

15. PROTECTION OF LEGAL SUBJECTS – Under the current object-oriented approach, authorities can only obtain data stored abroad through the slow international cooperation channels. Criminals can easily abuse this system by shrewdly using cloud services or by storing their data in countries that are known to be difficult in providing international cooperation.[18] To some extent, they can also circumvent the law of their countries by storing illegal content on servers located in countries where such content is not prohibited. Pseudo-child pornography comes to mind here: such material does not involve actual children, and it is not currently punishable in the same way in all countries.[19] Due to the fact that dual criminality can be a determining factor in the willingness of states to offer each other legal assistance, the criminal can manipulate this so as to seriously hamper criminal investigations.[20] A legal subject can choose to withdraw data from the competence of his authority by storing them abroad while enjoying full access and use of that data. Allocating the territorial competence for search exclusively to the state from which the consulted service is provided would involve a similar problem. In our view, the subject-oriented approach could restore the balance between the individual and the authority in this regard. Focusing on habitual residence ensures that the most important competencies of control of both the virtual and the physical life are vested in one and the same state. Individuals can no longer escape from the local legal system by storing data abroad, whilst enjoying full access and use of that data. It is only in this manner that the respective state can efficiently fulfil its entrusted task of controlling and protecting the legal subjects on its territory.

16. STATE OF RESIDENCE: PREFERENCE – It appears from the above comparison that the state where the investigated subject has his habitual residence should be given an autonomous investigative competence with regard to remote search for stored data. The autonomous investigative competence relates to the investigated subject's legal virtual environment. Making this competence dependent on the will of the state of storage or the service provider's state should, in our opinion, be excluded. As is the case with investigations in real time, the focus should be on the subject. However, it is the location of his place of residence, and not his personal location, that is decisive. Moreover, in a subject-

---

[18] G. VACIAGO, "Remote forensics and cloud computing: an Italian and European legal overview", *Digital Evidence and Electronic Signature Law Review*, 2011, vol. 8, 124.

[19] For example, in the United States, virtual child pornography is only punishable to the extent that it cannot be distinguished from real child pornography. See Prosecutorial Remedies and Other Tools to end the Exploitation of Child Pornography Today Act (PROTECT Act), *Pub. L.* No. 108-21, 117 Stat. 650 (2003); M.J. HENZEY, "Going on the offensive: a comprehensive overview of internet child pornography distribution and aggressive legal action", *Appalachian Journal of Law* 2011-12, vol. 11, 23-24. Far-reaching punishment of virtual child pornography has in the past already been labelled as unconstitutional in the United States. See *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002); Art. 383 *bis* of the Belgian Criminal Code, in contrast, makes pseudo-child pornography punishable by using more general terminology: "[...] symbols, objects, films, photographs, slides or other image carriers depicting positions or sexual acts of a pornographic nature, in which minors are involved *or are depicted* […]". Also merely accessing child pornography, without possessing it, is punishable in accordance with Article 383 *bis* § 2 of the Criminal Code.

[20] For example, Article 5 of the CoE Convention on mutual assistance in criminal matters provides: "*Any Contracting Party may […] reserve the right to make the execution of letters rogatory for search or seizure of property dependent on one or more of the following conditions: (a) that the offence motivating the letters rogatory is punishable under both the law of the requesting Party and the law of the requested Party […]* "; see also Art. 14 Council Framework Decision of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters.

oriented approach, legal subjects are given the protection they expect.[21] Regardless of where the data are to be found, the human rights of a person are protected on the basis of the law of the country where he has habitual residence and, in general, where he habitually consults his data. In this way, every virtual action falls within the scope of a coherent and, for the person concerned, familiar system of protection of privacy and other human rights. This also ensures that there is legal certainty.

3. Virtual searches in general: supplementary to the principle criterion?

17. OTHER STATES WITH WELL-FOUNDED LINK – We can conclude that the location of the subject and the location of his habitual residence must apply as principle criteria in locating virtual searches. The question still remains whether the competence of the subject state or residential state must be further supplemented by a territorial competence of other states with well-founded links with the sought data.

A. Service provider's state

18. SOVEREIGNTY - We are of the opinion that to deny the service provider's state the competence to autonomously investigate the data linked to that service could infringe its sovereignty. If the data sought are accessible to the service provider and are linked to its service, which is consulted by the investigated subject, the service provider's state displays a well-founded link with the data sought and its claim to sovereignty cannot merely be brushed aside. However, data passing through the infrastructure of a service provider do not, in itself, display a well-founded link with the service provider's state. In our opinion, there must be clear indications that the service was consulted by the investigated subject and that the sought data are related to the subject's use of the service.

19. LEGAL PROTECTION AND LEGAL CERTAINTY - If a legal subject uses services offered by a foreign service provider, he could also expect that his data can be investigated under the service provider's state's law. By using a service provided from abroad, the legal subject virtually transcends the borders of the territory where he is physically present. The investigated subject is not only physically present in one state, but also virtually enters the territory of another state from where he consults services. He must accept the consequences of transcending borders. He personally subjects his data to the sovereign competence of the state from where the service is provided. Consequently, legal certainty does not present any obstacle for this autonomous investigative competence. We therefore propose that the subject-oriented approach be supplemented with a competence that is based on the place from where the service consulted by the investigated subject is provided. The practical criteria to determine this place must reflect the focus on the subject. Which territory can the subject be presumed to have entered? This must in any event be a place known to the subject.

B. State of storage

20. SOVEREIGNTY - A lack of autonomous competence on the part of the state of storage can constitute an infringement of its sovereignty. (see no. 14) Here, too, we continue to approach the issue from the perspectives of legal protection and legal certainty. A distinction is needed here regarding to who stores the data abroad.

---

[21] See also the following text regarding the question on a shifting of the focus from the place where the data are stored to the place where there is an interference in fundamental rights and freedoms: F. CAJANI, *Technologies and Business vs Law - Cloud computing transborder access and data retention*, 2012, 16-17, www.coe.int.

21. STORAGE BY THE SERVICE PROVIDER - Under the first scenario, the service provider stores data in a foreign country without the express and clear permission or consent of the owner of that data. The state where the service provider stores a subject's data should not be allowed to derive any autonomous competence from such storage with regard to the subject's data. Let us explain why. A person must recognise that the sovereignty of his own state is limited and that there are other sovereign states that also have autonomous competencies to be able to fulfil their task of maintaining order and protecting their own territory. Consequently, the legal subject must recognise that when he decides to transcend his own state's borders, he thereby accepts the sovereignty of the state of the territory on which he decides to stay. However, the decision to transcend the borders and to subject himself to a foreign sovereign institution must, in the first place, lie with him personally. If the service provider (e.g. Google) has control over this by storing the legal subordinate's data in a place that is financially more viable, it becomes difficult to the subject to know which state has competence over his data and legal certainty in a virtual environment is therefore eroded. Moreover, the extent of the protection of human rights is then made to fully depend on the place where the service provider chooses to store the data. Cloud computing would only exacerbate this problem, because this involves storing data in different places and moving them around. In view of legal certainty and the protection of human rights, the competence of the state of storage must in this case be dependent on the cooperation of the subject state/state of habitual residence (depending on the type of investigation) or the state from where the service consulted by the subject is provided.

22. STORAGE BY INVESTIGATED SUBJECT - Under the second scenario, the investigated person himself stores the data in the foreign territory. Every time a legal subject personally stores his data on a specific server across borders, such storage subsequently involves the competence of the state of storage. This is the case, for example, when a person who has his habitual residence in Belgium, but works in the Netherlands, stores his data remotely on the servers in his office in the Netherlands. In this example, both Belgium and the Netherlands have autonomous investigative competence regarding the data stored in the Netherlands. Belgium has the competencies to perform a virtual search on the grounds of the principle criterion (habitual residence) and the Netherlands has the same competencies on the grounds of the supplementary criterion (the place where the subject stores his data). In all cases, the focus is on the investigated subject and on the question as to whether he virtually transcends borders and thereby subjects himself to the competence of a foreign state. This approach guarantees that the autonomous investigating state always displays a well-founded link with the investigated subject to whom the data relate or to whom they actually belong.

4. Proposal: cyberspace as virtual territory

23. VIRTUAL TERRITORY - We are of the opinion that we can conclude from the above that the focus on the subject and his virtual transcendence of borders should enjoy preference if we want to maintain territorially delineated sovereignty and the legal protection that is intended by it. This is why we propose that various authorities may have at their disposal autonomous competences to investigate the same virtual data, each on the grounds of a well-founded link between its physical territory and the investigated subject and his data. Consequently, we find that the territoriality principle is still feasible. A symbolic representation can explain what we are proposing. We can take the Internet as

what it is: a network of networks,[22]as a *res communis*, like the high seas.[23] Everyone is allowed to use it, but is required to have due regard to the general interests that it serves. However, everything that happens there bears one or more flags.[24] Such a flag is indicative of an adequately well-founded link between the data and the physical territory of a certain state. All data bearing the flag of a certain state jointly form the *virtual territory* of that state. The metaphor of *virtual territory* clearly reflects how we wish to delineate the sovereign competence of a state in cyberspace. Although, at first sight, this wording seems to be a contradiction in terms, it may help to visualise the proposed approach. The virtual territory is an extension of the physical territory and is inextricably linked to it. Consequently, not only does every state have sovereign competencies within its physical territory, but it also has sovereign, albeit often shared, competencies within its virtual territory. In this way, investigative acts performed on a state's virtual territory fall within its territorial spheres of competence.

24. COMPONENTS VIRTUAL TERRITORY - The virtual territory of a state contains of (1) the data related to the virtual past of its residents, as far as those data are legally accessible to those residents (cf. searches for stored data), (2) data related to real time activities of legal subject located on its territory (real time searches), (3) data accessible to service providers present in its territory and related to services consulted by the investigated subject[25] and (4) data stored on a state's territory by the investigated subject. Finally, (5) data that are accessible to everyone, whether or not this is under nonrestrictive conditions, such as registration or payment, also constitute part of the state's virtual territory. There is currently already an international agreement in this regard (art. 32 Cybercrime Convention).

5. Applicability of the new approach

A. Practical steps forward

25. ACCELERATION OF CRIMINAL INVESTIGATION – We have already seen that the current object-oriented approach is particularly problematic because it necessitates a disproportionate reliance on slow international cooperation. The idea of a virtual territory would solve this problem and the criminal investigation could be substantially accelerated. In view of the fleeting nature of digital data, speed is of primary importance to secure proof.

26. COHERENT APPROACH TO THE LOCATING ISSUE – In our opinion, the subject-oriented approach coherently resolves the issue concerning the determination of the location of investigative measures. Traditional investigative competencies always require physical crossing of borders so that they can be performed abroad. However, with regard to criminal investigation, territorial limitation of state sovereignty excludes unilateral physical border crossing by law enforcement agencies. Wiretapping formed a first challenge to thinking in terms of territoriality. The physical crossing of borders was no longer essential to intercept a conversation of a person abroad. Furthermore, it is

---

[22] G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, kms2.isn.ethz.ch, 23.

[23] M. HILDEBRANDT, "Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal* 2013,vol. 63, 211.

[24] By way of comparison: W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds.), *4th International Conference on Cyber Conflict*, Tallinn, NATO CCD COE Publications, 2012, 9.

[25] It is important that the subject has consulted the service. The sought data may not be merely passing through the service provider's infrastructure purely for technical reasons.

difficult to determine where the data sought (the communication) are to be found. The European legislator did not explicitly address the locating issue but quietly shifted focus from the location of the evidence sought to the location of the investigated subject. In this way, a state only has autonomous competence to wiretap if the investigated person is on its territory. The Council of Europe later confirmed this approach partly in the Convention on Cybercrime for virtual search in real time. The focus on the subject for virtual searches proposed above, provides a coherent approach regarding investigations where there is no need to physically cross territorial borders because the evidence is directly available from the investigating state's territory. The location of the investigated subject or his habitual residence determines in the first place where the investigative competence is located. What is important in this respect is that the user also does not need to personally transcend the borders to consult the data. This competence must be further supplemented by the competence of the state whose territory the investigated subject enters virtually. There, too, the focus is on the subject. Therefor, an autonomous competence belongs to the state from where the internet services, consulted by the subject, are provided or the state where the subject stores his data. A technical coincidental presence of data (cf. Article 20 of the EU Convention on Mutual Assistance in Criminal Matters and art. 31 Directive European Investigation Order) or transborder storage by a service provider[26] is insufficient to establish investigative competence for the respective state in relation to the data due to the lack of a well-founded link with the investigated subject.

B. Problematic issues

a. Dependence on cooperation of the service providers' state

27. IDENTIFICATION AND DETERMINATION OF LOCATION THROUGH ISP – When law enforcement agencies want to look into data which are related to an online service and both accessible to the user and the service provider, the subject-oriented principle firstly vests sovereign competence in the state where the investigated subject is to be found or where his habitual residence is located (depending on the type of search). That competence is supplemented by the sovereign competence of the state from where the service consulted by the subject is provided. However, law enforcement agencies will often not know the location of the subject or his habitual residence. As long as these locations are unknown, the service state is the only state with autonomous competences to access the sought after data. Furthermore, in order to determine the location of the subject or his habitual residence, the cooperation of the same ISP is often essential. The investigation then strongly depends on the extent to which the service state is prepared to cooperate.

28. LACK OF COOPERATION - However, over-dependence on the cooperation of the state where the service provider is to be found is problematic. The investigation may become deadlocked when there is no cooperation. This enables the criminal to make use of services that are provided from states that are known to be difficult in providing international cooperation. In this way a criminal can personally contribute to the obstruction of a local criminal investigation. When the location or habitual residence of the investigated person is unknown, investigating institutions will feel compelled, in cases of anonymity and lack of international judicial assistance, to assume competence as subject state or state of residence.[27] As soon as there are serious indications at hand that the subject

[26] = The location of the data stored is under control of the service provider.

[27] As long as the investigating institutions do not know which state is the subject or residence state, it will not be known whose sovereignty is infringed. In our opinion, such an assumption of competence is also necessary when both the place

is to be found in a third state or has his habitual residence there (depending on the type of investigation), international rules regarding cooperation will be required once again.

29. SLOW COOPERATION – When the state of the service provider is indeed prepared to cooperate, such cooperation often takes too long. This is why efforts must be made to accelerate international cooperation in investigating a virtual environment. The already existing possibility of requesting a freezing order can offer a solution. However, in our opinion such request should be addressed to the state where the service provider is established.[28] When the requested state discovers that a service provider from a third state or from the requesting state was also consulted regarding the data sought (e.g. IAP (Telenet)), that state can immediately communicate the necessary traffic data to the requesting state so that the latter can be afforded the opportunity of securing all the data sought from all the service providers involved.[29] Both forms of cooperation can be refused when (1) the crime leading to the request for judicial assistance constitutes a political crime or is linked to such a crime, or (2) the requested state regards the freezing or communication as being contrary to its sovereignty, security, public order or other essential interests. However, it would be more efficient if service providers were to be directly approachable. The protection of human rights may however not be made subordinate to the efficiency of the criminal investigation. Yet, in our view, it should be possible and is advisable to impose on states the obligation to instruct their ISPs to directly answer to certain orders by certain foreign authorities.

30. DIRECT COOPERATION BETWEEN CONSTITUTIONAL STATES – Possible direct orders could firstly concern location. The ISP would be able to indicate to which country the IP address used refers without communicating the IP address as such. When it becomes apparent that the investigated subject acts on the territory of the investigating state or when the ISP has information that indicates that the investigated subject has his habitual residence on the territory of the investigating state, the ISP's direct approachability could be maintained. They could then directly communicate the IP address or assist the respective authority in its search for data. A direct freezing order could also be issued pending a more well-founded request to provide data. The states concluding the Convention would have to designate a national institution that could be authorised to directly address the ISPs. The other signatory states to the Convention would be notified of such a decision. In this way, abuse through a lack op authority can be avoided. However, we are of the opinion that direct responses to such requests for information must be subjected to the requesting state's respect for fundamental rights. With regard to the parties to the ECHR or equivalent legal instrument (in respect of both the content and the control system),[30] a refutable assumption of respect for fundamental rights could

---

from where the services are provided and the place where the investigated person is to be found or where he has his habitual residence is unknown. Example: an investigation into a criminal service provider through which a suspect establishes an illegal trading business. In our opinion, if only the place from where the service is provided is unknown, a state could also assume competence as a service provider's state if the cooperation of a state that has the competence on the grounds of another criterion is unworkable. In all cases, the investigation must firstly be aimed at determining the unknown factors.

[28] Cf. Article 29 of the Convention on Cybercrime, which provides the possibility of addressing a request for judicial assistance, requiring few formalities, to the state of storage for the freezing of the sought data, pending a more well-founded request to provide the data sought. (Explanatory report to the Convention on Cybercrime, no. 283). We are of the opinion that it is difficult to make a request to the state of storage practicable. As a matter of fact, investigating institutions will usually need the service provider's technical assistance to freeze data. Moreover, the state of storage is often unknown or the service provider's assistance is required to identify such state of storage. It therefore seems to us that a request to the state where the service provider is established is necessary.

[29] By way of comparison: Art. 30 Covention on Cybercrime.

[30] By way of comparison ECHR 30 June 2005, no. 45036/98, Bosphorus/Ireland, no. 155.

apply. For other countries, a list of states satisfying this request can be drawn up.[31] This could be an important incentive for states to provide efficient legal protection. Furthermore, a standard form could be provided that must be used by the designated investigating institutions in the requesting states to make their request, in which *inter alia* the suspected crime, the reason why the person is suspected and the necessity for the search should be indicated. The required information would be more limited for the freezing order than for the order to provide data.[32]

31. SUBSIDIARITY PRINCIPLE – Good accessibility on the part of an ISP is more important than it may seem on first sight. The subsidiarity principle, according to which the least drastic measure appropriate for the intended purpose has preference is, in our view, inherent to a system effectively protecting fundamental rights[33] Having regard to this principle, preference should be given to direct consultation of the ISP or to international cooperation above, for example, a national competence to hack into computer systems[34] (e.g. mailbox of a subject having his habitual residence in the investigating state) if the same result can be achieved in this manner. However, that preference only applies if the direct consultation or international cooperation also works effectively. If direct access (such as hacking) is the only way to attain a satisfactory result, the investigating state shall feel compelled to use that competence if the conditions in accordance with the national law are satisfied.

b. Loss of subject-location

32. ANONIMISING TOOLS – Anonimising tools pose an additional problem. Even if investigating institutions succeed in procuring the necessary IP address by means of the cooperation of an ISP, it is still not certain whether they can actually locate and identify the investigated subject. All types of publically available tools, such as proxy servers[35] or The Onion Router (TOR)[36] in fact enable internet users to conceal their identity. It is then difficult, if not impossible, to trace not only the identity, but also the location of the respective person. Investigating institutions will therefore only be able to continue to operate in cooperation with the country where the service provider consulted by the investigated subject is to be found or the country where the subject is seemingly (but not actually) to be found.

33. SERIOUS SIGNS OF ANONIMISING TOOL - In any event, we argue that states must be able to act unilaterally if there are serious indications that the subject is using anonimising tools. This should only be possible if the cooperation of the state of the service provider consulted by the investigated subject cannot provide a solution. It will not be possible to know which sovereignty is infringed by

---

[31] By way of comparison: art. 25 and 26 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See also art. 40 proposal General Data Protection Regulation.

[32] With regard to the freezing order: art. 29, 2 Convention on Cybercrime.

[33] See in the framework of art. 8 ECHR: P. DE HERT, *Art. 8 EVRM en het Belgische recht*, Gent, Mys & Breesch, 1998, 42.

[34] With regard to hacking competence, see: Art. 126 nba Dutch legislative proposal to amend the Criminal Code and the Criminal Procedure Code on improving and reinforcing the tracing and prosecution of computer criminality, https://www.rijksoverheid.nl/ National hacking competence can also present problems, however, if the state where the hacked system is to be found regards this as criminal access to the computer system. See C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 30. This problem arises because of the difference between the proposed locating principles in Criminal Procedure and the current locating principles in substantial Criminal Law. However, the reciprocity principal can lead to states tolerating such action. Clear international agreements are advisable, however.

[35] See, for example www.proxy4free.com.

[36] See D. GOLDSCHLAG, M. REED, P. SYVERSON, *Onion Routing for Anonymous and Private Internet Connections*, Communications of the ACM, February 1999, vol.42 No. 2, 39-41; See also the article "HTG explains: Is Tor really Anonymous and Secure", http://www.howtogeek.com.

the continued performance of the investigation as long as the investigating institutions do not know which state is the state of residence or the subject state. That is why investigating institutions should be able to assume competence. However, they should make every effort to firstly discover the location of the subject or his place of residence (depending on the type of investigation). As soon as there are serious indications that the subject is to be found on the territory of a third state or has his habitual residence there, said state's sovereignty must be respected. Making any other assessment would profoundly disrupt the balance between individuals and the state. In this way the individual would in fact have too much power to hinder a criminal investigation.

C. Summary

34. DETERMINING COMPETENCE: HOW THIS WOULD WORK IN PRACTICE – The diagram below helps to determine whether, based on our proposal, a state's investigating institutions are territorially competent and, therefore, can conduct a criminal investigation in accordance with their national laws. It also indicates when it must/can obtain cooperation from another state, and which state that may be.

The questions in the diagram must always be answered on the basis of *serious indications*.

- Definitions:
    - The subject is the (legal) person in respect of (which) whom the investigative act is performed. This is not necessarily the suspect.
    - The notion "data" always refers to the data sought by the investigating institutions.
    - The service provider (SP) must always be a SP that is consulted by the subject. Merely transmitting data through the SP's channels is insufficient.
    - The concept "accessible" refers to legal access.
- All options must always be pursued. *Therefore, there may be various final solutions* (e.g. various possibilities for cooperation).
- State X, Y and Z must be identifiable states. As long as this is not the case, the answer to the question is "unknown".
- If, after having pursued the various possibilities, "competent" is reached, one can unilaterally start searching for the data for which purpose the diagram was applied.
- If one of the possibilities is "assuming competence", all other results must first be considered. Competence can only be assumed if these other results are not practicable. When competence is assumed on the basis of an unknown factor, the investigation must primarily be aimed at identifying the unknown factor. The diagram must be gone through again as soon as there are serious indications that allow the unknown factor to be filled in.
- When there are serious indications that anonimising tools are being used, the questions can also be answered as they seemingly appear to be, in addition to the option provided.

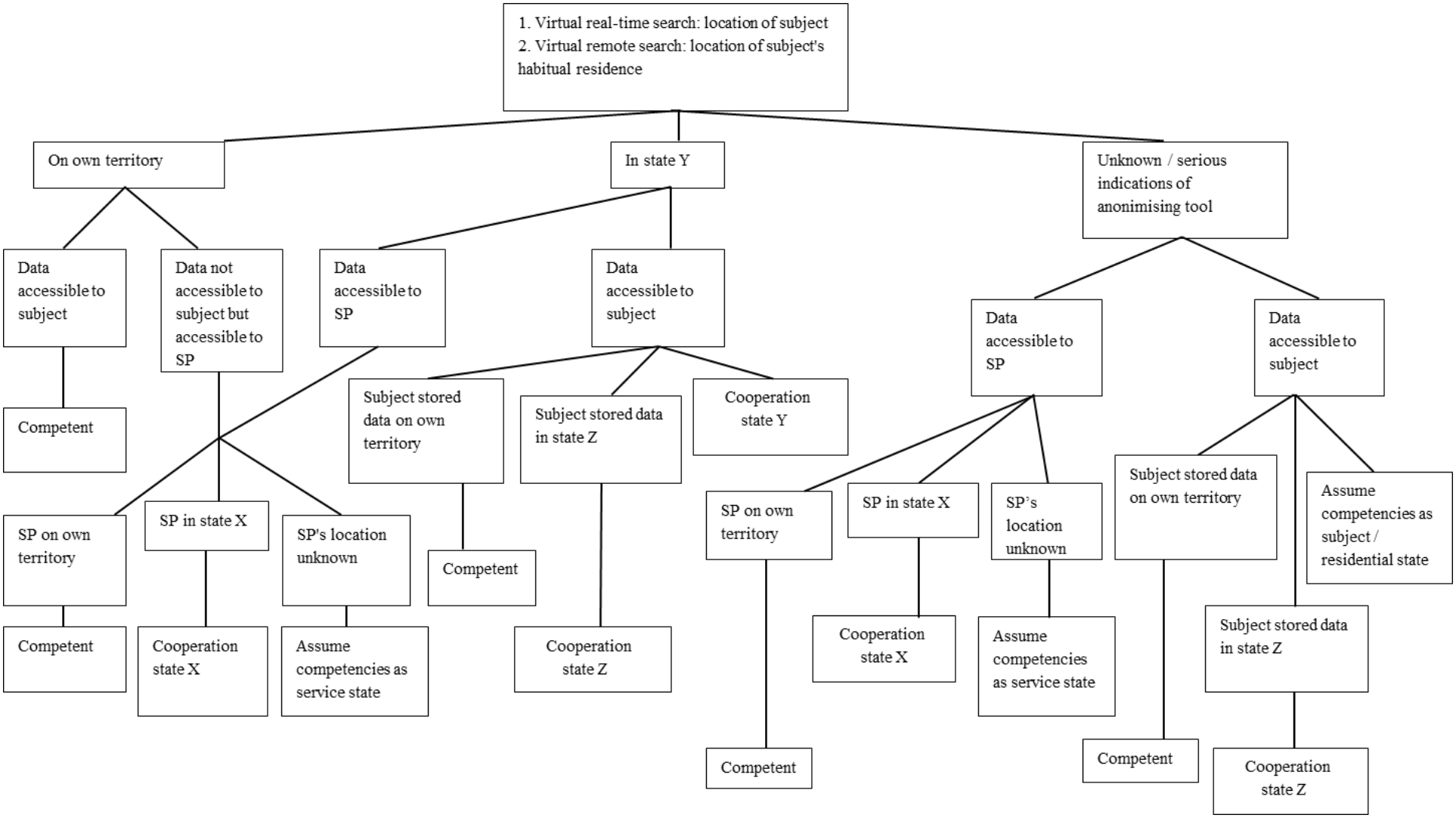

Figure 1: Diagram of territorial competence/need for cooperation for virtual search.

Conclusion

The territorial limitation of state sovereignty restricts the competence of investigating institutions to their own territories. The question regarding how we must locate investigative acts territorially has not yet been explicitly and unequivocally answered in international and national law. The place where the investigative acts take place is often self-evident. However, it is more difficult to answer that question when the location of the sought evidence is unclear or the place where the evidence is to be found is not the same as the place of access to the evidence. Digitisation of the world and, therefore, also of possible evidence, presents us with serious challenges.

If we want to sustain the territorially limited sovereignty and the legal protection intended by it, we must put the focus on the investigated subject in order to locate virtual investigative acts. That approach is particularly innovative for searches relating to data stored at a distance. In this regard, national and international legislators (provisionally) opt for a focus on the place where the sought data are stored. However, we are of the opinion that this focus is based on a logical error. The object-oriented approach, with which we are currently working, is a further development of the locating principle applied to searches for physical evidence. However, this approach may not and cannot be blindly applied to the virtual remote search. Not only does the object-oriented approach infringe the sovereignty of the state where the data are being consulted by the subject, it also undermines the legal protection intended by conferring territorially limited sovereignty to states. Moreover, the current approach appears to be unworkable in practice.

We are of the opinion that the subject-oriented approach is imperative to secure state sovereignty, legal certainty and protection of fundamental freedoms and human rights. Focusing on the subject also benefits the efficiency of the criminal investigation, although this entails particular problems that states will be required to face primarily by means of practical international agreements. Depending on the type of investigation, the place where the subject is to be found or the place where he has his habitual residence determines competence. In addition, the investigated subject's virtual crossing of borders also entails competence. Such crossing of borders is involved when the investigated subject consults foreign services or stores data on particular servers abroad. The extremely large need for legal assistance is in this way replaced by direct access for investigative institutions to their sovereign state's virtual territory. However, one question still remains unanswered: Are we ready for thinking in terms of virtuality in our legal system?