

INTERNET EVIDENCE

- NEW METHODS

The use of Internet monitoring and web crawler tools
in collecting and preserving evidence
in bias-motivated cases.



stowarzyszenie
żydowskie
czulent



Foundation
EVZ Remembrance
Responsibility
Future



Powering solutions
to extremism
and polarisation



Coalition to Counter
Online Antisemitism

With support from [Google.org](https://www.google.org)

Copyright © by Jewish Association Czulent

Publisher

Jewish Association Czulent

ul. Sebastiana 36/1

31-051 Kraków

www.czulent.pl

office@czulent.pl

Kraków 2024

Edition I

ISBN: 978-83-972977-2-2

Substantive Editing: Joanna Grabarczyk-Anders

Drawn up by: Jakub Kłosiński, Jędrzej Kupczyński

Free publication, not for sale.

Publication under the CC BY-SA 4.0 PL

Support our organisation by donating to our account:

Jewish Association Czulent

ul. Sebastiana 36/1

31-051 Kraków

NIP (tax ID): 6762300850

Account No.:42 1600 1462 1880 9351 6000 0001

This publication has been produced within the framework of the project "New Methods of Gathering Evidence on antisemitic crimes committed on Social Media" funded by the The Coalition to Counter Online Antisemitism (CCOA).

This publication has been produced within the framework of the project "Online antisemitism in Poland: establishment of a legal aid helpdesk, reporting and advocacy activities", funded by the Foundation Remembrance, Responsibility and Future (EVZ), and implemented by the Jewish Association Czulent.

This publication does not present the position or views of the Foundation Remembrance, Responsibility and Future (EVZ) and The Coalition to Counter Online Antisemitism (CCOA).

Table of Contents

5	Introduction
7	Introduction – computer data as evidence in criminal proceedings
7	Definition and features of digital evidence
8	Polish legal basis – computer data treated analogously to objects under Article 236a of the Code of Criminal Proceedings
9	International legislation: DSA and the Council of Europe Convention on Cybercrime
11	The type and scope of data processed by online platforms, including “social media” providers
11	Categories of data processed by online platforms
12	Data Retention Period for Online Platforms
12	Online platforms’ data retention periods
12	Access to user-deleted data
13	Examples of data processing policies of popular network service providers: FB, X, TikTok
13	Facebook
14	X
15	TikTok
15	What information can be derived from the data processed by online platforms, and how to determine a user’s identity from it?
18	Difficulties and problems related to establishing user identity from IP address and how to counteract them

20	Access to data processed by online platforms for law enforcement agencies
20	Introduction
21	Choosing the right form of international cooperation
21	International legal assistance request
22	European Investigation Order
22	Voluntary data release by its controller
25	Scope of data available from the user's device – in the context of online platforms
26	The evidentiary significance of information obtained and secured using web crawling and big data software
26	Introduction
26	Characteristics of indexing robots (web crawlers)
26	SentiOne's performance characteristics
27	Use of a network monitoring report in criminal proceedings on the example of SentiOne
29	Is the credibility of the report in doubt?
31	What findings can be made based on the report?
34	Actions of the judicial body after reviewing the report
35	Inspection by the judicial body
35	Obtaining information from site administrator
36	Making a copy of the page
36	Wayback Machine
36	Notary certification of page content
37	Rules for formulating evidentiary motions
37	Introduction
38	To whom should an evidentiary motion be directed?
39	Formulation of facta probanda
40	How do law enforcement agencies handle an evidentiary motion?

1 | Introduction

Crimes motivated by prejudice strike at the foundations of equality and social security. Their victims – whether individuals, organizations or entire groups of people – experience not only psychological damage, but also social exclusion and fear for their own safety. Responding to such incidents is crucial in providing support to those affected and protecting minority communities from escalation of threats. Failure to take appropriate action could lead to the normalization of hatred in the public space, which is unacceptable.

There has been a disturbing trend in recent years – a steady rise in the number of hate crimes on the Internet. Social media, discussion forums, as well as other digital spaces, instead of promoting exchange of ideas and networking, are becoming a tool for spreading hate speech, or even waging mass attacks on individuals, organizations and groups, especially the minority ones.

One of the most important steps in the fight against hate crimes is to inform law enforcement of their occurrence.

In the era of rapid Internet development, we are not able to manually monitor all incidents. This is why content analysis and monitoring tools such as SentiOne are becoming increasingly important. They make it possible to detect and document organized hate campaigns, as well as gather evidence in cases of cyberbullying or violations of personal dignity. These technologies play a key role in documenting legal violations, especially when their perpetrators remain anonymous.

This publication is a guide to the world of new technologies and using them to help bring the perpetrators of bias-motivated crimes committed on the Internet to criminal justice. It also shows how organizations can use evidence from commercial tools, regularly used for promotional purposes and for checking effectiveness of marketing efforts (social listening), to inform police and prosecutors about crimes committed against them. This publication is also a guide for attorneys, police officers

or prosecutors on how to use digital evidence from crawling tools.

The publication is based on years of experience in monitoring hateful content, supporting victims in the process of collecting evidence, and notifying of possible crimes committed by unidentified persons. The material we prepared was created thanks to the knowledge and experience of the Jewish Czulent Association and the expertise of the prosecutors. The practical tips presented in the study are based on proven methods and real-life cases, which makes them an effective tool in the fight against hate crimes on the Internet.

Together – using technology, legal support and responsible response – we can help create a safer digital space for all.

2 | Introduction – computer data as evidence in criminal proceedings

Digital evidence is crucial in modern criminal proceedings. They are estimated to occur in up to 85% of criminal proceedings conducted in Europe¹.

Definition and features of digital evidence

Digital evidence (electronic evidence, e-evidence) can be defined as any type of information of evidentiary significance recorded or transmitted in electronic form². In practice, this term can include very diverse types of data, such as, for example: the content of communications (e-mail, SMS, instant messaging); data of a subscriber or user of electronically provided services (e.g., data presented when registering an account on Facebook or X platform); or, finally, network traffic data (information about the IP address from which an Internet session during which evidentially significant events occurred was established), and others.

Depending on the type of data, they are controlled by various entities: individuals, companies and corporations, public entities. What is important from an investigative perspective is that the same data can sometimes be accessed by law enforcement agencies in several ways. For example, the content published by a user on a social network can be obtained and secured for prosecution purposes both from an open source of information, i.e. directly from the Internet (as long as the user makes it available to the public), from the provider of the social media in question, or from the user themselves, when access data to their account is obtained from them or electronic devices on which the user remains logged into said account are secured.

1 European Commission, COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT

2 The CEELI Institute, Toolkit for Handling and Admissibility of Electronic Evidence

Moreover, the law enforcement agencies' ability to acquire data from network service providers is sometimes significantly hampered, whether due to lack of cooperation, the absence of instruments allowing to actually force foreign entities to exchange the information, the limited scope of voluntary data exchange and the significant lengthiness of international legal assistance procedures. On the other hand, even securing electronic devices directly from the user does not automatically open up access to all data stored on those devices, or in related network services. However, proactive action by the victim or notifier taken yet before the criminal proceedings are initiated can effectively secure at least some evidence for later proceedings.

Polish legal basis – computer data treated analogously to objects under Article 236a of the Code of Criminal Proceedings

The Criminal Procedure Code contains no explicit definition of digital evidence or electronic evidence. This, however, is not an oversight. While the Code regulates how to conduct basic, typical evidentiary procedures (such as questioning a witness, obtaining an expert opinion, etc.), it does not contain a closed catalog of evidence. On the contrary, it is assumed that evidence may be anything permitted by criminal procedural law as long as it contributes to findings having bearing on a procedural decision³.

Article 236a of the Code of Criminal Proceedings, contained in Chapter 25 dealing with seizures and searches, is crucial here. According to Article 236a of the Code of Criminal Proceedings the provisions on seizure of property and search shall apply accordingly: “to the holder and user of a device containing electronic data or an IT system, with regard to the data stored on such device or in such system or on a data storage medium in their possession or use, including correspondence sent by e-mail”. Thus, the Code uses the term “computer data” and prescribes for it to be treated analogously to physical items that may be secured in the course of a search or seizure.

“Computer data,” as referred to in Article 236a of the Code of Criminal Proceedings, includes in practice all types of information recorded and processed on electronic devices and in computer networks. For such data to be obtainable for the purposes of criminal proceedings it must be determined that it constitutes evidence in the case (Article 217 § 1 of the Code of Criminal Proceedings, in conjunction with Article 236a of the Code of Criminal Procedure), and for telecommunications data, that it is “relevant to ongoing proceedings” (Article 218 § of the Code of Criminal Procedure). Obtaining this data requires an order from the prosecutor or the court (at the stage of judicial proceedings).

3 T. Grzegorzcyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 2001, s. 435.

International legislation: DSA and the Council of Europe Convention on Cybercrime

European legislation defines “electronic evidence” as subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form. A “service provider” in this definition is simply an entity that provides electronic communication services, various online applications and services or services related to the administration of Internet domains. This definition is included in the e-evidence regulation⁴, which, although already enacted, will not come into effect until August 18, 2026.

It is impossible to talk about computer data processing on the Internet without discussing the EU DSA (Digital Services Act⁵). It is directly applicable in individual EU Member States (it does not require legislative implementation). It does not define “computer data,” focusing instead on a slightly different concept – “intermediary service”. In practice, it means transmitting, storing and making available (including making available to the public) information, data, content and messages from Internet users.

Moreover, the DSA defines “online platforms” as services meant for storing user-sourced data and disseminating it to the public. In practice, therefore, social media – platforms such as Facebook, X, TikTok – fall under the DSA as “Internet platforms,” and their providers are required to comply with the provisions of this regulation. Particularly stringent regulations apply to “very large online platforms” (“VLOPs⁶”), i.e. those with an average of at least 45 million active users per month within the European Union.

While the DSA is mainly concerned with the way the digital services market is administered, the so-called Budapest Convention (the Council of Europe Convention on Cybercrime⁷) and its additional protocols were designed directly to combat computer crimes, including those related to racism and xenophobia. The latter issues are specifically addressed by the First Additional Protocol to the Convention. Poland has ratified both the Convention and the Additional Protocol.

4 European Commission, European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

5 European Commission, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ 2022 L 277/1

6 The full list is available on the website European Commission

7 Convention on Cybercrime of the Council of Europe, adopted in Budapest on 23 November 2001

The Budapest Convention defines “computer data” broadly, as any representation of facts, information or concepts in a computer system. The Internet is a type of “computer system” as defined by this convention. The First Additional Protocol obliges to criminalize a number of behaviors related to, for example, distributing racist and xenophobic materials in a “computer system,” threatening and insulting people through a “computer system” on the basis of racial or ethnic origin, etc., denying genocides and crimes against humanity⁸, etc.

8 A detailed description of the acts that, according to the Additional Protocol, should constitute crimes can be found in Articles 3-7 of the protocol. It is worth noting that Poland ratified this protocol with two reservations. Specifically, Poland invoked the reservation that the distribution of racist and xenophobic materials will constitute a crime only if such materials incite discrimination associated with violence or hatred. Additionally, the denial or endorsement of genocide or crimes against humanity will constitute a crime only if accompanied by an intention to incite hatred, discrimination, or acts of violence against an individual or a group.

3 | The type and scope of data processed by online platforms, including “social media” providers

Categories of data processed by online platforms

Online platform providers process a very wide range of computer data regarding users. In the most general terms, it can be divided into two categories: content data (concerning the content) and non-content data (other data).

The first category includes the content published, posted or uploaded by users of the service, such as text in a Facebook post, a photo uploaded to Instagram, a video posted on YouTube, as well as the content of electronic correspondence exchanged between users of email inboxes or instant messaging services such as Messenger, WhatsApp, Signal or Telegram⁹.

The second category (non-content data) includes:

1. Subscriber/user data – that is, all data identifying the customer (Internet user) and the service they use. For example, for a Facebook user, this would include: first name, last name, phone number and other data provided when registering an account, data on payments made by the customer to Facebook, but also technical data, e.g. regarding user’s devices associated with that account and data related to verifying the customer’s identity (which would be more relevant for financial services such as online banking and payment services). Importantly, however, this category does not include passwords or other means of authentication that replace passwords. So while law enforcement agencies generally can obtain subscriber data, they will not thus obtain passwords for the user’s services or platforms.

⁹ It is worth noting that in the case of Telegram, exchanging messages between two users is just one of its features, alongside discussion groups, groups dedicated to posting announcements, and „channels” with characteristics similar to microblogs.

2. (Network) traffic data – is essentially data related to electronic communications. The most important – from the point of view of effective investigation – are the IP address and network port number of the user of the Internet service, along with the exact date and time (including seconds) when the connection to that service was established. For example, if a user posted a comment under a YouTube video, the network traffic data would primarily mean the IP address of the device from which he or she was connected to the Internet while writing that comment, along with the network port number, as well as the exact date and time when he or she connected to the YouTube platform. But that’s not all. The network traffic data may also include a range of further information related to the user’s connection, such as the user’s location, software features and the models of devices used for the connection. Such detailed data, however, is not necessarily recorded by all service providers.

Data Retention Period for Online Platforms

As previously mentioned, telecommunication data is generally retained for a period of 12 months (in Poland). This is explicitly mandated by the Telecommunications Law¹⁰. However, this obligation applies exclusively to telecommunication companies (such as network providers like Plus, Play, T-Mobile, Orange, etc.) and not to online platforms or other network services.

Online platforms’ data retention periods.

How long do online platforms keep data? It depends on the policy of the specific platform. Basically, the data is stored for as long as it is needed to provide the user with a particular function or service. That being said, in practice the platform’s decision whether to store or not to store the data relies primarily on business concerns. So, typically user data is kept as long as its processing can generate economic benefits for the platform.

Access to user-deleted data

Access to user-deleted data looks similarly, both from the user’s and law enforcement’s perspective. Individual platforms and other Internet service providers may individually shape their policies regarding storage of such data, e.g. in the case of an email service, deleted messages are most often still stored in a “trash” folder and are only deleted after a manual “deleting the trash” or at the end of a time specified by the service provider.

¹⁰ Telecommunications Law

Final deletion of such data by the user most often makes it unavailable to law enforcement agencies as well, even if such agencies properly request them from an online platform or other provider. On the other hand, the provider may specify certain events to trigger further storage of data, despite their deletion by the user. This may occur, for example, in the event of a suspected violation of the rules of an online platform – while the administrator verifies the occurrence of the violation. **Some providers may also stipulate that a manual deletion of data by the user does not at all mean that the data is fully removed from the platform’s servers, but only makes it inaccessible to other users.**

Examples of data processing policies of popular network service providers: FB, X, TikTok

Facebook is owned by Meta corporation, as is Instagram, Messenger and WhatsApp. X, formerly Twitter, now connected to Elon Musk, is owned by X Corp, the US-based company he founded. TikTok’s ownership structure is a bit more complicated, but it is ultimately owned by the Chinese company ByteDance Ltd. based in Beijing, although formally registered in the Cayman Islands.

[Facebook¹¹](#)

As a rule, the platform processes user data for as long as they are needed to provide services and functionality. What does this mean in practice? This depends on the category of data and the specific situation. User account login data, photos and posts published by the user (which have not been deleted) are stored for the entire lifetime of the user’s account. However, Facebook also records the history of user’s activity on the platform. Meta corporation keeps such data for 6 months, unless manually deleted. If a user manually deletes content (posts, photos), they are available in Facebook’s “trash” folder for 30 days. Afterwards the automatic removal process begins. In practice, this process (which includes deleting data also from backup and disaster recovery systems) can take up to 90 days. The deletion process will begin sooner if the user manually deletes the trash. However, the provider of Facebook has taken good care to “hide” the trash on the platform’s website, so presumably not all users are even aware of its existence nor of the possibility to empty it manually¹². During the 90-day removal process, they will most likely already be unavailable to law enforcement agencies, even if they approach the Meta corporation in the proper manner.

¹¹ Developed based on Meta corporation’s documentation current as of November 2024.

¹² On the platform’s homepage on a computer, you need to select the tile with the profile picture in the top left corner, then „Privacy Settings,” followed by „Activity Log,” and finally, in the menu on the left, search for „Trash.”

Deletion of an account by the user automatically initiates a process of deleting all user data, which can take up to 90 days. In this situation, user data can be retained by the platform only if the law stipulates that such obligation exists. If, for example, law enforcement agencies or a court in an appropriate procedure request the Meta corporation to freeze specific data of a particular user, the deletion of the account by that user will not result in deletion of the data by the platform – the data will be stored until the end of the “freeze” period.

X¹³

The retention period for X also depends on the type of data and the individual case. Profile data and login data are stored for the entire lifetime of the account. User-published content, comments, interactions with other users are also available throughout the lifetime of the account, unless manually deleted. X stores the IP address used to connect to the platform, as well as other network connection parameters, for a period of 13 months. Information about the content viewed by the user, including the ads they click, is available for 90 days. However, all or part of these types of data may be kept longer if X’s administrator is verifying a possible violation of the platform’s rules and regulations or suspends the account, or if external legal obligations exist.

On the X portal, users can both delete individual¹⁴ posts and deactivate the entire account. Currently, the platform does not have the functionality to delete multiple posts at once. And what happens to deleted posts, can they be recovered? Unlike Facebook, platform X does not contain a “trash” folder, and deleting a post has an immediate effect and results – as the portal administrator declares – in its removal from: the user’s account, the timeline of users following that account and search results on the platform. That is, such a post will become invisible to users of the platform. X’s administrator, however, happens to leave out information about whether the content of the post would also become unavailable to the very administrator. In practice, therefore, it is difficult to know whether by manually deleting a post the user actually deletes it on X’s servers, or merely prevents it from being displayed from the users’ side. However, even if this was the case, law enforcement agencies’ ability to access already deleted posts is rather doubtful.

Deactivating an account has no practical effect on the data associated with that account for the first thirty days. This is because during this period the user can log in again, which will be equivalent to reactivating the account. Only upon expiration of this 30-day period will the account be permanently

13 Developed based on the X administrator’s documentation current as of November 2024

14 <https://help.x.com/en/using-x/delete-posts>

deleted. Then, the user's private messages and public profile will also be unavailable. However, X's administrator will keep "certain" data about the deleted account (the administrator does not specify in their documents what data that would be) for security purposes.

Similarly to Facebook, law enforcement's request to freeze the data will protect it from deletion even if the user later decides to delete it manually.

TikTok¹⁵

Again, the retention period depends on the type of data and the specific situation. That being said, TikTok's privacy policy is worded in a rather concise manner – one can learn little more than that user data is kept for "as long as necessary to provide services." Only by way of example: for data categories including: account information (user data and login information) user-published content; messages – the platform administrator states that it stores them for as long as the user's account is active. There is no information on how long user's platform login information, such as IP address and related connection parameters, is available.

Removal of individual pieces of content by a TikTok user is possible. In such a case, however, the data is not immediately deleted, but continues to be stored for a period of "up to 30 days," known as the grace period. During this period, the data can be viewed in the recently deleted folder, retrieved and restored to the user's account. It would therefore also be available to law enforcement agencies.

TikTok offers users the option to delete their account or deactivate their account. The former implies irrevocable loss of the user's account. Deactivation, on the other hand, is the suspension of an account with the possibility of reactivation. In this case, user data is not deleted at all. Potentially, then, law enforcement agencies may have access to it. The type, scope and timing of TikTok's deletion of user data are unclear in the case of account deletion – the platform's documents do not specify them. However, it should be assumed that in this case the data will no longer be available to law enforcement agencies, even if they apply to TikTok through the proper procedure.

What information can be derived from the data processed by online platforms, and how to determine a user's identity from it?

Sometimes users publish content on the Internet under their full, real name. If that is not the case,

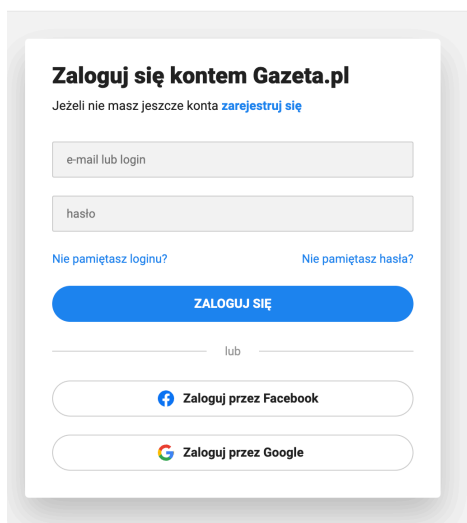
15 Developed based on the X administrator's documentation current as of November 2024.

the identity of the author of a given post, comment, entry, video, etc. has to be determined from subscriber and network traffic data processed by the online platform.

The easiest, but also the most unreliable way to determine the identity of a user of a given content is for law enforcement agencies to obtain the subscriber data mentioned above. Why is it unreliable? It is important to remember that a user who publishes, for example, a comment under a video on YouTube does not at all have to provide their real data when registering on the platform. And sometimes one user's account can be used by a completely different person. So, stopping at subscriber data may be insufficient to establish the real identity of the author. On the other hand, many network services allow users to register and subsequently log in "through Facebook," "through Google," or using another existing user account in another service. In such case the two accounts get linked. This can be advantageous for determining a user's identity, because the account used to authenticate in a new network service often happens to be one that the user uses in everyday life, and to which their real data, and possibly other information leading to the detection of their identity, is associated.

Example. Suppose an article on Gazeta.pl website had a racist comment. A Gazeta.pl account is necessary to post comments under articles. One can register an account "manually" – providing login, e-mail and password. But it is also possible to log in by linking to one's Facebook or Google account. If the user took advantage of this opportunity, the racist comment they published may be traceable to their Facebook or Google account. Chances are that they use these accounts on a daily basis and that the accounts contain their real data. Even if they don't, these accounts may still contain information that makes it easier to detect their identity, such as photos with their image published on Facebook, information about their circle of "friends," or, last but not least, the payment card details associated with the account.

Konto



The screenshot shows the login interface for Gazeta.pl. At the top, it says "Zaloguj się kontem Gazeta.pl". Below this, there is a link "Jeżeli nie masz jeszcze konta zarejestruj się". The main form has two input fields: "e-mail lub login" and "hasło". Below the fields are two links: "Nie pamiętasz loginu?" and "Nie pamiętasz hasła?". A large blue button labeled "ZALOGUJ SIĘ" is positioned below the form. At the bottom, there are two buttons for social media login: "Zaloguj przez Facebook" and "Zaloguj przez Google".

Figure 1. Screenshot from konto.gazeta.pl – two ways to log in to the account: via login and email or via one of the linked accounts: Facebook or Google (access date: 30 November 2024)

And if the user provided false data and did not take the opportunity to link the account? This is why IP address data is so important. “IP” stands for Internet Protocol. It is a string of digits (or digits and letters in the case of version six of the IP protocol) that:

- identifies an individual device connected to a network, e.g. the Internet;
- at the same time indicates which company is the Internet provider for a particular connection.

Let’s use an example to discuss this. An example IP address (in version four of the IP protocol – which is still the most common) might look like this: 188.146.23.68¹⁶. Let’s assume this is the IP address used by the user who published the comment of interest on YouTube. To decipher the data it contains, you need to use one of the analytical tools available online, such as CentralOps¹⁷. Analysis of this address will give the following result:

The screenshot shows the CentralOps.net website interface. The main heading is "Domain Dossier" with the subtitle "Investigate domains and IP addresses". A search bar contains the IP address "188.146.23.68". Below the search bar, there are several checkboxes: "domain whois record" (checked), "DNS records" (checked), "tracertool" (unchecked), "network whois record" (checked), and "service scan" (unchecked). A "GO" button is visible. The user information section shows "user: anonymous [79.191.92.159]" and "balance: 49 units". A message box states: "To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [more information]". The "Address lookup" section shows the canonical name "188.146.23.68.mobile.internet.t-mobile.pl" and the address "188.146.23.68". The "Domain Whois record" section shows "Queried whois.dns.pl with 't-mobile.pl'..." and "DOMAIN NAME: t-mobile.pl".

Figure 2. A screenshot from centralops.net after IP address analysis: 188.146.23.68 (Access date: 20 November 2024)

What is the result of the analysis performed? That the user of IP address 188.146.23.68 uses an Internet connection provided by T-Mobile. Internet providers can be either telecommunications operators, e.g. network providers: Plus, Play, T-Mobile or Orange (in which case we are talking about so-called “mobile Internet”) or entrepreneurs providing Internet to homes or offices, e.g. UPC, Vectra, etc. (so-called “fixed-line Internet connection”).

¹⁶ An IP address in version six of the protocol could look like this, for example: 2001:0db8:0001:0000:0000:0ab9:COA8:0102.

¹⁷ Available at: centralops.net. Alternatives include, for example: <https://www.whois.com/>; <https://whatismyipaddress.com/>; <https://ip-lookup.net/> and many others.

After getting that far, there is only one step left to learning about the identity of the person who used the Internet connection. In this step the law enforcement authorities obtain, from a telecommunications operator or another Internet provider, the details of a customer with whom a contract has been entered into under which that customer made connection to the Internet using a specific IP address. In our example that means the specific subscriber who is using the telecommunications services provided by T-Mobile, under which they established a connection using IP address 188.146.23.68.

By enquiring the Internet service provider (by means of an order issued by a prosecutor or a court) law enforcement authorities will obtain information about a specific person (their first and last name) who used a particular IP address.

Difficulties and problems related to establishing user identity from IP address and how to counteract them

The previous paragraph optimistically assumed that the author of the analyzed YouTube comment is exactly the same person who entered into a telecommunications services contract with T-Mobile, under which they established an Internet connection from IP address 188.146.23.68. However, this does not have to be the case at all.

1. A phone number¹⁸ registered to a certain person may in fact be used by another person: a family member, an acquaintance or even a complete stranger.
2. The user of the phone number can either share the Internet with another person or place the SIM card in a router, thus creating a WiFi network based on the mobile connection.
3. This can also be the case with fixed Internet connection: the same WiFi network can be used by a larger group of people like family, household members, office employees, etc. An IP address essentially identifies the router¹⁹ from which WiFi users connect the Internet, not the device (computer, phone) that connects to that router. This difficulty can sometimes be overcome. The router records (in so-called logs/system logs) information about when and what devices connected to it, in order to connect to the Internet. Thus, having access to the router, you could determine which specific device established a given connection to the Internet. On the other hand, it should be

18 Precisely – it is the SIM card that is subject to mandatory registration, not the mobile phone number referred to by the acronym MSISDN.

19 Precisely – to access the user panel/interface for managing a given router, knowledge of the password is required. However, it is worth noting that many users never change the default password for the user panel, making it easy to guess (it typically depends on the router's manufacturer and model, and is often something like „admin” or a similar variation). Many users are unaware of the option to change the password for this panel. Access to the user panel is obtained by entering the specified address or IP address, usually provided by the router manufacturer on a label located on the bottom of the device. This information, along with the default password, can also typically be found on the router manufacturer's technical support website (e.g., <http://tplinkwifi.net/>).

noted that, depending on the router model and user settings, logs may be stored only for a limited period of time, may be “manually” erased by the user, or may be erased due to router shutdown (e.g. during a power outage).

4. Moreover, if a user connects to an open WiFi network (in a public place, coffee shop, airport, etc.), the IP address will only identify the entity that provided the open WiFi network and not the specific user connecting to the network (although some public WiFi networks may require an email address or other data in order to provide an Internet connection; in such cases it may be possible to establish the identity of the user; this depends on whether the user has used data that is actually linked to their identity, and whether this data is still available at all from the network administrator).
5. Users can use software to mask their identity on the Internet, such as VPN (Virtual Private Network) or TOR (The Onion Router). In both cases, an Internet connection is established via other devices with different IP addresses than the device from which the connection was actually established. “Deanonymization” of a user who has used a VPN is theoretically possible if this data is obtained from the VPN service provider but this is difficult to achieve in practice. “Deanonymization” of a TOR network user requires specialized analysis of network traffic data at a level that is completely unattainable in most criminal cases.
6. If the telecommunications data retention period (which is 12 months in Poland) has expired, the telecommunications operator will not be able to identify the user by the IP address (this applies to “mobile Internet connection”).
7. Unambiguously identifying a device that connects to the Internet by a “mobile link” (provided by a telecommunications operator) requires knowing not only the IP address, but also the network port number. However, some Internet service providers (including online platforms) do not collect network port number data at all. This problem does not exist when using “fixed Internet” connection.

4 Access to data processed by online platforms for law enforcement agencies.

Introduction

In the course of criminal proceedings, a judicial body (e.g., a police officer, a prosecutor or a court) collects evidence, some of which can be obtained without any formalized procedure (e.g. attaching photographs provided by the victim to the file), while some requires compliance with the provisions of the Code of Criminal Proceedings and other laws. For example, obtaining telecommunications data (e.g. the list of connections of a given MSISDN number during a given period or the data of a subscriber with a specific IP address assigned) can be done only on the basis of a court or prosecutor's order and only when the interest of administration of justice requires it.

When evidence relevant to criminal proceedings is located outside the Republic of Poland or its holder is a foreign entity, its acquisition is carried out under special rules. Choosing the right way to obtain evidence will depend on three factors:

- first, on the country where the evidence in question is located (e.g. where the witness who needs to be interviewed resides; where the C2 server used in the attack is located; where the mobile network operator whose services the perpetrator used to post relevant content online is based; where the headquarters or branch office of the entity administering the online platform on which the content was posted is located). This is because different legal acts will apply to European Union countries and to third countries. In the case of some countries, the chance of obtaining any data within a reasonable period of time will be slim to none;
- second, on the type of evidence to be conducted. Some data categories require special formalities; for example, the prevailing view is that obtaining data subject to banking secrecy from a foreign bank requires first obtaining the permission of a Polish court to provide information subject to secrecy, and only then applying to the competent authorities of the other country. Other data can be obtained without any formalities, e.g. if a country offers the possibility of reviewing the court registry through a publicly accessible government website, data obtained from such a service

may constitute evidence in Polish criminal proceedings. Given the vast amount of information collected in publicly available records, in many cases it may turn out that a basic OSINT analysis (i.e. identification from publicly available sources) will avoid a lengthy wait to obtain data from another country's authorities;

- third, on the policies of a given entity, such as an online platform. Administrators of some services refuse to release any data to representatives of other countries, and as a consequence, authorities of the country in which the entity is located need to be approached, following appropriate procedures. Subsequently, the authority of that country obtains the data and transmits it to be used in Polish criminal proceedings. Other platforms, on the other hand, take a more liberal approach, providing foreign government representatives with data as sensitive as, for example, the credit card number used to pay for a service or the full details of the cryptocurrency wallet holder, often without even requiring any formal request: email correspondence from an address on a government domain may be sufficient.

Choosing the right form of international cooperation

International legal assistance request

The basic way to obtain evidence located abroad or at the disposal of a foreign entity is to submit an international legal assistance request to the authorities of the country in question (depending on the country: to the central authority, such as the relevant ministry, or to the judicial body, such as the prosecutor's office). Such request is sometimes referred to as MLAT, as it originates from a mutual legal assistance treaty. The location of the entity that is the holder of the data we want to obtain for criminal proceedings is crucial for choosing the right procedure.

It is worth taking the time to determine:

- where the entity from which we want to obtain evidence is located. It is necessary to determine the exact, current address, since sometimes after waiting for months for legal assistance, the judicial body receives a response that the entity is not located at the indicated address. Court registries, for example, which are available online in many countries, can be helpful for this purpose. It is also worth establishing all possible forms of contact, including email addresses, phone numbers and even contact forms: there is no obstacle for foreign service officers who will be performing legal assistance to attempt to make contact by such non-standard means if necessary;

- whether the entity in question has the data we are interested in. For example, a platform may adopt a policy that, depending on the category of evidence to be issued, the request should be addressed to its headquarters or to a field branch located in another country. Getting familiar with the rules of cooperation of a platform can prevent a situation where a request is submitted to a wrong country, leading to wasted time and even data loss.

European Investigation Order

In relations between European Union Member States, with the exception of Ireland and Denmark, legal assistance requests have been replaced with European Investigation Orders (EIOs). This legal act allows for simplifying and significantly speeding up the obtaining of evidence within the EU, among other things, due to the fact that the EIO is addressed directly to the judicial body rather than to the central authorities. It also facilitates direct contact (e.g., by email) between the prosecutor or judge issuing the warrant and the officer who executes it.

The Judicial Atlas tool is available on the European Judicial Network portal (<https://www.ejn-crimjust.europa.eu/ejn2021/AtlasChooseCountry>), which makes it easy to determine to which authority the EIO should be submitted in a given case.

Voluntary data release by its controller

In many cases, it is not necessary to submit an EIO or a legal assistance request, even though data relevant to criminal proceedings are administered by a foreign entity. More and more platforms ensure the provision of information to foreign judicial bodies without the intermediation of domestic authorities. There may be restrictions in this regard, e.g. the non-content data will be provided by a given platform based on an order issued by a foreign prosecutor or court, while the content data is reserved for domestic authorities and a legal assistance request is needed to obtain it. It should be emphasized that, contrary to the opinions sometimes expressed by representatives of Polish judicial bodies, the data obtained in this way, “unofficially” so to speak, without the intermediation of a foreign authority, constitute full-fledged evidence. There is no rational reason to treat an email containing certain data, sent directly to a Polish authority, as less valuable than if it had been obtained through the execution of a legal assistance request.

Facebook (Meta Platforms)

Cooperation with judicial authorities within the Facebook platform has been dispersed among different organizational units, depending on what the inquiry concerns. According to information made available by the administrator:

- with respect to Facebook platform users in the European Union, information is provided by Meta Platforms Ireland Ltd., Law Enforcement Response Team, Merrion Road, Dublin 4, D04 X2KP, Ireland (not applicable to Traffic and Content Data, i.e. data on traffic, profile content, message content, etc.);
- with respect to payments through Meta Pay made in the European Union, information is provided by Meta Payments International Limited, Legal Department, Merrion Road, Dublin 4, D04 X2KP, Ireland;
- with respect to Facebook platform users in the U.S., as well as Traffic and Content Data regardless of the user's location, information is provided by Meta Platforms Inc., 1601 Willow Road, Menlo Park California 94025, USA;
- with respect to payments through Meta Pay made in the U.S., information is provided by Meta Payments Inc., Legal Department, 1601 Willow Road, Menlo Park California 94025, USA.

Some of the data, including information about the IP addresses from which the profile was logged into, email address, phone number, as well as the user's name and date of birth, is provided by the administrator through the Law Enforcement Online Requests System (LEORS) panel. The panel can be accessed by any representative of a judicial body (including a prosecutor, judge, police officer), using a personal email address in the gov.pl domain. By default, a scan of the order (e.g. on the release of legally protected secrets) is required to be attached to the request and there is no need to translate it into English. However, it is also necessary to fill out a form in English with a brief description of the reasons for the request.

It is worth pointing out that in practice the current level of responding through LEORS greatly limits the routing of requests to Meta Platforms Ireland Ltd. because if any information is not available through LEORS, i.e. it falls into the Traffic Data or Content Data category, it is necessary to direct a legal assistance request to the US authorities to obtain the information from Meta Platforms Inc. Requests to Meta Platforms Ireland Ltd. will therefore be limited to Preservation Requests, i.e. requests for data preservation, and Emergency Disclosure Requests, i.e. requests for disclosure of information in emergency situations, although such categories of requests can usually be recognized through LEORS, which includes relevant tabs.

On the other hand, within the Traffic Data and Content Data categories, it is possible to obtain a very wide range of information, almost exhausting the data catalog held by the administrator on a given user. However, some information is deleted after a certain period of time, while other information is retained for as long as the user's account is maintained. More detailed data in this regard cannot be published in a presented available study.

Unless the judicial body wants the user to be notified of an inquiry about their profile by state authorities, it should be stipulated in the form or legal assistance request.

Instagram (Meta Platforms)

On the Instagram platform, information is provided to the judicial bodies by the same entities as on the Facebook platform, i.e. Meta Platforms Ireland Ltd, Meta Payments International Limited, Meta Platforms Inc. and Meta Payments Inc, with the division of tasks identical to Facebook.

Also, the scope of data shared through voluntary cooperation and international legal assistance is the same as for the Facebook platform. The same panel, LEORS, is used to submit direct requests to the platform administrator, so all comments on its operation, indicated in the Facebook platform description, are up-to-date.

Unless the judicial body wants the user to be notified of an inquiry about their profile by state authorities, it should be stipulated in the form or legal assistance request.

WhatsApp (Meta Platforms)

WhatsApp messenger has different channels of communication with judicial bodies than the other Met platforms. User data is administered by the following entities:

- in the case of users from the European Economic Area, i.e. EU and Norway, Switzerland and Liechtenstein: WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland
- in the case of users in other areas: WhatsApp LLC, 1601 Willow Road, Menlo Park, California 94025, USA

The LEORS (Law Enforcement Online Request System) panel, available at <https://www.whatsapp.com/records/login>, is used for obtaining information as part of voluntary cooperation with judicial bodies.

The scope of information provided by the administrator does not include in any case the content of messages exchanged between users.

Data security

To conclude this section of the study, it is worth mentioning the possibility of the judicial body to request that data be secured for a period of up to 90 days, which should be sufficient for the authority to draft and translate an official request for legal assistance/EIO. Such an obligation results from the Council of Europe Convention on Cybercrime (the so-called Budapest Convention), Articles 16 and 29.

The period for which an entity will keep data pending an official request for its release depends on national law and the policy of the company in question (for example, Meta provides for a period of 90 days, and it does not delete data until the user profile is deleted) but the convention provides for a period of no less than 60 days. It should be assumed that in a situation where data is not shared based on voluntary cooperation with judicial authorities (and thus a request for legal assistance/EIO is required), there is always a risk of data loss. Therefore, it may be considered good practice to precede such a request/EIO with a request (e.g. in the form of an email or by selecting the appropriate tab in the form for judicial authorities) for data security under the Cybersecurity Convention.

Scope of data available from the user's device – in the context of online platforms

As signaled in the introductory section, the data published on social media essentially “resides” on the servers of the providers of these services, in data centers located in various places around the world, rather than in the memory of individual users' devices. However, there may be copies of this data or temporary files containing this data, possibly data backups, on personal devices (computers, phones). The scope of data available from a device is not uniform and depends on both the technical solutions used by a particular platform and the user's privacy settings and personal configurations. It is therefore difficult to provide general principles.

One might be tempted to say that instant messaging, as a rule, stores a copy of the conversation “locally”, that is in the device memory. This means that conversations on such communicators as: Messenger, WhatsApp, Signal, even Telegram, or on messengers associated with, for example, TikTok, Instagram, SnapChat, will often be accessed from the user's device (provided, of course, it proves possible to “unlock” that device).

5 | The evidentiary significance of information obtained and secured using web crawling and big data software.

Introduction

The source of information about online activities bearing the hallmarks of criminal acts, including hate crimes, may be not only publications spotted by representatives of judicial bodies or other Internet users, but also, on a much larger scale, posts or comments selected by so-called crawlers, i.e. indexing robots (bots).

Characteristics of indexing robots (web crawlers)

The task of crawlers is to automatically extract website content, which is preceded by an analysis of the given website. Crawlers are the backbone of search engines, but this is not their only purpose: depending on the goal for which a robot is tailored, it can collect specific data categories.

Analysis of large datasets published on the Internet relies heavily on the operation of indexing robots. Some are designed to search for user-designated content on social networks or online forums. It is therefore easy to imagine their potential use by entities that analyze network resources for published content with hate speech characteristics, such as social organizations. In this study we will analyze the opportunities and challenges of using such tools in criminal proceedings. The commercial tool SentiOne will be used as an example.

SentiOne's performance characteristics

The product in question, which belongs to the Polish company SentiOne sp. z o.o., is used for monitoring Internet resources (social listening) for the purposes of marketing campaigns or PR activities, among others. Using machine learning algorithms based on powerful training data, the tool allows, among other things, to select online publications containing specific keywords, as well as to group

them according to the sentiment of the statements, distinguishing between positive, neutral and negative statements.

For example, it is possible to check the occurrence of a specific keyword (e.g., “Poles”) on circled dates. The search result can be narrowed down to specific platforms (Facebook, Instagram, X, TikTok or Reddit) or specific site categories, such as portals, forums, blogs, reviews, videos. The resulting entries can be grouped by category, for example, limiting further analysis to those statements that were rated as negative by the program.

It is worth noting at this point that indexing robots, as a rule, only collect public content, so they do not have access to, for example, entries published in closed groups or posted by users who apply visibility restrictions to their posts.

You can finish your work with the SentiOne tool by generating a report containing the selected statements. It is possible to imagine the use of such a report when filing a criminal report, involving the publication of content bearing the hallmarks of criminal acts, such as those specified in Article 256 of the Criminal Code, so a discussion of the related practical issues is necessary.

Use of a network monitoring report in criminal proceedings on the example of SentiOne

The report can include the full content of a given entry, along with the date and time of publication and author designation. In the case of a newspaper article or a blog post, the person signed under the text is indicated as the author. The report may also indicate the lack of data about the author. In the case of a post or comment on social media, the name of the profile from which the content was published is presented. Tweets posted on the X platform are additionally accompanied by a personalized handle.

It is worth noting that the acquisition of data by web crawling software from social media platforms is most often done using the IT infrastructure provided directly by the administrator of such a platform for the needs of big data analytics entrepreneurs, such as, for example, the provider of SentiOne.

There is no doubt that the report can serve as a prelude to further collection of materials for criminal proceedings. For example, the comments, tweets or publications that incite hatred on the basis of national differences selected in it can then be traced back to the source sites. The notifier or a representative of the judicial body may consult the content of a given profile on a social media platform

and confirm that a given post exists, which will lead to further evidentiary procedures aimed at recording the content of the post and establishing the identity of the person who published it. In such a situation, the report generated using SentiOne is first and foremost a starting point for the collection of evidence that will come from the source sites, so even if the judicial body decides that a private document in the form of a report cannot form the basis of factual findings, it will fulfill its role, because it will be treated not as evidence, but as information about evidence that will then be obtained from the relevant platforms.

It is worth noting that the acquisition of data by web crawling software from social media platforms is most often done using the IT infrastructure provided directly by the administrator of such a platform for the needs of big data analytics entrepreneurs, such as, for example, the provider of SentiOne.

There is no doubt that the report can serve as a prelude to further collection of materials for criminal proceedings. For example, the comments, tweets or publications that incite hatred on the basis of national differences selected in it can then be traced back to the source sites. The notifier or a representative of the judicial body may consult the content of a given profile on a social media platform and confirm that a given post exists, which will lead to further evidentiary procedures aimed at recording the content of the post and establishing the identity of the person who published it. In such a situation, the report generated using SentiOne is first and foremost a starting point for the collection of evidence that will come from the source sites, so even if the judicial body decides that a private document in the form of a report cannot form the basis of factual findings, it will fulfill its role, because it will be treated not as evidence, but as information about evidence that will then be obtained from the relevant platforms.

The situation is markedly different if it turns out that a particular entry appearing in the report had been removed before it was secured in any other way for the purpose of criminal proceedings. If the report generated from SentiOne is the only confirmation that a certain content was published on a given profile, the question to be resolved is whether this can constitute sufficient proof of such fact.

When answering this question, it is first necessary to once again refer to the principle of free evaluation of evidence, which is in force in the Polish legal order, resulting from Article 7 of the Code of Criminal Proceedings:

The proceeding authorities form their conviction on the basis of all the evidentiary proceedings carried out, which are evaluated freely taking into account the principles of sound reasoning and indications of knowledge and life experience.

The principle of free evaluation of evidence is one of the pillars of Polish criminal procedure and Article 7 of the Code of Criminal Proceedings has been subject to numerous monographs and sections of commentaries. Its interpretation also takes into account the very extensive jurisprudence of the courts. It is impossible to summarize all this scientific and jurisprudential output in a few sentences for the purposes of this publication. However, it is necessary to relate the principle in question to the possibility of using specific evidence, which would be a report generated using the SentiOne tool or any analogous document showing the result of the indexing robots' activities.

First of all, such a report can constitute evidence in criminal proceedings, just like almost any other object or record of content (with certain exclusions, specified, among others, in the Code of Criminal Proceedings, outside of the subject of this study). The admissibility of this type of evidence in criminal procedure is confirmed by Article 393 § 3 of the Code of Criminal Proceedings, according to which it is possible to read at trial any so-called "private documents", i.e. those created outside the proceedings, produced by private parties.

If the report is obtained in the course of the proceedings (e.g. provided to the prosecutor by the notifier), it is subject to assessment by the judicial body: at the stage of investigation or inquiry it is the prosecutor or police officer or a representative of another authority, and at the stage of jurisdictional proceedings it is the court. As part of this evaluation, the authority will determine, among other things, whether the evidence in question was obtained legally, whether its credibility raises no doubt, and what factual findings can be made based on it (in other words, what results from the evidence). The legality of the evidence in the form of the report in question should not raise any doubts, as it is a compilation of content published on the Internet, without any restrictions on access by third parties. However, more attention should be paid to the other two issues.

Is the credibility of the report in doubt?

In other words, if the original content has been irretrievably deleted and there is no way to obtain it through any other means, can a report resulting from a crawler act as proof that specific content was posted on a particular profile/page?

In the opinion of the authors of the study, this question should be answered in the affirmative, with the proviso, however, that only the totality of the circumstances of a given case will determine the possibility of using the evidence in question to make findings of fact, that is, to determine the course of the relevant events that are examined in criminal proceedings.

In the opinion of the authors of the study, this question should be answered in the affirmative, with the proviso, however, that only the totality of the circumstances of a given case will determine the possibility of using the evidence in question to make findings of fact, that is, to determine the course of the relevant events that are examined in criminal proceedings.

The report includes content downloaded in an automated manner from publicly available social media profile pages and websites. This content is not modified, i.e. shortened, supplemented or edited, in any way. Using artificial intelligence algorithms to generate the report also has no effect on content authenticity assessment, as it only selects content and categorizes it in terms of what sentiment the statement expresses (negative, neutral or positive). Of course, how the algorithm classifies a given utterance is completely irrelevant to the findings of the investigation procedure. The judicial body will make its own assessment of what the intention of the author of the post was, and it will be responsible for determining, for example, whether the post is ironic or mocking, which may not have been reflected in the report.

When faced with potential problems that may arise in the course of criminal proceedings, it is worth examining the question of whether the judicial body should take any additional steps to establish that the content generated in the report has not been modified. For example, is it necessary to analyze how the algorithms used by SentiOne work to be able to establish that they only download content, without modifying it? For this purpose, is it necessary to consult an expert who will examine the entire process of generating the report and express their opinion on the immutability of the extracted content?

It should be noted here that it is common practice for judicial bodies to base their findings on technical solutions that the authorities do not know or understand. This statement is not, despite appearances, critical; rather, it refers to the specifics of operating in an environment of dynamic information technology development. For example, in the course of a particular proceeding, it may be determined that a message relevant to the process was sent to a particular e-mail inbox from another address. The judicial body will take steps to establish that such a message actually reached the addressee (e.g., it will inspect the addressee's e-mail inbox), and that the address of the sender of the message is not in doubt (e.g., it will examine the extended header or, if it has the opportunity, it will examine the outbox from which the message was sent). If the conclusions of these activities are clear, the authority will make a factual finding that a message of a certain content was sent from outbox "A" to inbox "B". However, it can be taken for granted that in almost all cases, a representative of a judicial body (e.g., a police officer, prosecutor or judge) has very limited knowledge (if any) of what technical solutions were used to ensure that a message sent from one account reaches another account unaltered.

At the same time, the authors are not aware of any cases in which a judicial body has entertained a doubt in this regard, i.e. that, absent special circumstances, it had a doubt that the content of the message sent by the sender reached the recipient in an unaltered form. The authority's doubts do not relate to the technical solutions used by e-mail administrators, but to entirely different issues, such as whether it is possible to determine who was using the sender's e-mail account at the time the e-mail was sent.

This example, like any analogy, has some weaknesses. It does not correspond to the situation under analysis in every aspect, i.e. the issue of immutability of content published in the SentiOne report. In particular, it must be borne in mind that e-mail is used on a daily basis by the vast majority of the population, so the representative of the judicial body, even if they had no knowledge of the technical solutions used, knows the principle of its operation from their own experience. The same cannot be said for the use of crawlers extracting data from social networks – this technology is not widespread enough for the average judicial body representative to have any opinion about it. On the other hand, however, similar examples can be formulated in abundance, e.g., if a certain photo is posted on a social media profile page, it is assumed that the person with (authorized or unauthorized) access to the profile posted the photo; if a person is listed as another person's contact on a certain instant messenger, it is assumed that they must have been added to the contacts by that person. In none of these types of cases do the judicial bodies decide to obtain an expert opinion to resolve any doubts arising from a lack of knowledge of the technical solutions used in a given application.

On the other hand, it might be a good idea for the notifier or judicial body to ask the administrator or the developer of the particular program generating the reports about issues of concern to the body, such as whether the content in the reports is modified in any way. Obtaining an answer, possibly supported by a description of the technical solutions used, should be sufficient to confirm this key point.

What findings can be made based on the report?

Depending on the service package selected, SentiOne offers analysis of historical data going back up to three years. At the same time, the delay in data collection is very small, i.e., a crawler can include in its report posts published only a few seconds earlier. This means that as long as the post in question contains the keyword indicated by the user, was publicly available and was posted at any time during the three years prior to the generation of the report (even if it was removed shortly thereafter), it should be included in the report as a rule. The users' experience shows that false-negative results are possible, i.e., that the report does not include a post that was available during the monitoring period,

while there is no possibility of false-positive results, i.e., that the report includes posts or publications that were not actually posted by the user in question. The latter feature of the reports is crucial to their usefulness in criminal proceedings, since a finding that the reports may provide erroneous results would preclude the use of the report as independent evidence of the fact that certain content was published. Such consequences are not brought by the occasional omission from the reports of some entries deleted by the author, which may be due to the nature of crawlers.

Thus, the report not only allows for automated search for content that meets specific criteria, but also makes it easier to put it into context. It is possible to use the tool in question to analyze individual profile pages, so you can easily demonstrate that a particular content published on a specific profile page, bearing the characteristics of hate speech, is not incidental, but is accompanied by a lot of content of a similar nature. This result can also be achieved by manually checking the content of the profile (a crawler does not reveal any content that is not available to other users of a given platform), but the use of analytics tools helps speed up the process. This is especially important if there are a lot of posts on the analyzed profile page.

Analytical tools, such as SentiOne, also show relationships between different profile pages more efficiently, which can help determine that they are administered by the same entity or by individuals acting in concert or according to the same plan or guidelines. For example, narrowing down the period covered by the analysis and searching for specific keywords will show that very similar content was published on different profile pages in a short period of time. This should provide an impetus for further research, which may show that such a situation (duplication of content in a small interval on multiple accounts) occurs regularly, which may lead to the conclusion that these profile pages are related, e.g. by virtue of being created by the same person.

Such observations will be important in criminal proceedings, where it is always necessary to establish the intent and motivation of the perpetrator of a given act. In each case, it will affect the socially harmful consequences of the act, which also translates into the possible sentence. Moreover, in some cases, the identification of the perpetrator's purpose determines whether a particular act constitutes a crime. For example, public propagation of Nazi or communist ideology constitutes a crime under Article 263 § 1a of the Polish Criminal Code only if it is intended to influence political or social life. Finally, it is worth recalling that most of the acts specified in the Polish Criminal Code constitute a crime only if they are committed intentionally. Therefore, establishing the context of the statements, uncovering other examples of similar content being published, or demonstrating acting in concert with another person posting the same posts can be critical to a successful prosecution.

At the same time, however, it must be remembered that the report (accepting the argument presented in the previous section as to the authenticity of the posts listed in the report) proves only one thing, namely that a post with a certain content was posted on a certain profile page on a certain date. In any case, this is not sufficient to conclude that a person has committed a crime, even if the profile page in question can be linked to a specific person without any doubt. Indeed, criminal proceedings will require dealing with potential difficulties, which, depending on the facts, may include:

- ruling out the possibility that the post was published by someone other than the established account holder (although it is worth mentioning that making the account available to another person for the purpose of enabling them to publish a post bearing the hallmarks of a crime can be treated as aiding and abetting the crime, and under certain conditions even as complicity);
- establishing that the account holder did not lose access to the account, for example, as a result of a hacking attack (this is not a purely theoretical threat – the authors of this study are aware of criminal proceedings conducted in connection with social media posts which were subsequently found to have been posted after the security to the account had been breached or bypassed for the purpose of criminal proceedings being initiated against the holders of these accounts);
- demonstrating beyond a reasonable doubt that the account in question is maintained by a specific person; this must take into account the possibility that the creation of the account, or even its maintenance over a long period of time, may have constituted a sophisticated provocation aimed at damaging the reputation of the person in question, or even at bringing criminal proceedings against them. The authors of the publication are familiar with the example of the creation of a fake profile of a public official, bearing his name, surname and photo, to publish content for a certain period of time to show unequivocally that its author was the aforementioned official, and then begin publishing racist content. This action did not lead to criminal proceedings against the aforementioned person, however, it significantly damaged their reputation.

Criminal proceedings, of course, require the resolution of many other doubts, including the state of the perpetrator's awareness, their motivation, their sanity, and others, but this is beyond the scope of this paper. Thus, the data contained in an Internet monitoring report can significantly contribute to determining what content has been published on a particular profile page, but it is merely a starting point for further investigation that may ultimately result in attributing a crime to a specific person.

To conclude this section of the paper, it is worth returning once again to the fundamental question – is the credibility of the report beyond doubt? As indicated previously, the answer is affirmative in the authors' opinion, but only taking into account the realities of the specific case. Indeed, while there is no doubt that the report generated by SentiOne or other monitoring tools does not alter the content

retrieved by the indexing robots (and thus reflects the actual content of the posts or comments), it is difficult to imagine a situation in which a single post found in a monitoring report removed from a given site before procedural safeguards were implemented could constitute the only and sufficient evidence to bring charges against a person. This is because it is necessary to deal with all the doubts that arise along the way between the complaint of a criminal offence and the issuance of a sentence, only some of which were described above, and which would be extremely difficult to resolve based on the network monitoring report alone.

Actions of the judicial body after reviewing the report

As already signaled, the Polish Code of Criminal Proceedings provides for very few restrictions on the admissibility of evidence, and it can be pointed out, in simple terms, that almost all materials that the notifier is able to present to the judicial body or that the judicial body is able to legally obtain can be put into evidence (exceptions to this rule are provided for, inter alia, in Articles 171, 174, 178 and 178a of the Polish Code of Criminal Proceedings). Thus, evidence can include a media monitoring report containing an online publication, a screenshot of a comment posted on a social network, or even the testimony of a witness who recounts having read a comment of a certain content on a particular portal. The regulations do not provide for a gradation of evidence, and it is impossible to conclude in isolation from the realities of a particular case that a particular category of evidence will prevail over evidence from another category.

At the same time, however, any evidence may be considered by the judicial body as useless – although admissible – if it is not possible to make findings of fact on its basis beyond a reasonable doubt. For example, the aforementioned screenshot may be challenged by a user of a given profile, who claims that they have never published such content. If a screenshot, generally representing a very low value due to the possibility of fabrication or manipulation of an authentic screenshot, is the only evidence to prove that a comment was actually published, it is reasonable to assume that the court will not consider such evidence sufficient to establish this fact. In other words, while almost any evidence is admissible, not all of it represents any value in criminal proceedings. If another participant in the proceedings (or the court, acting on its own motion) is able to undermine the credibility of the evidence in question or the possibility of drawing certain conclusions from it, it may not have any impact on the factual findings.

Advice on how to strengthen the evidence that will be introduced into criminal proceedings so as to reduce the risk of undermining it and make it easier to draw clearer conclusions based on it is presented below.

Inspection by the judicial body

The natural inclination of a police officer or prosecutor, upon learning that a particular website contains content with the hallmarks of a crime, is to verify this by visiting the site. Once it has been determined that the site under investigation does indeed contain content relevant to the criminal proceedings, the officer usually proceeds with an inspection, i.e., they take a look at what the site looks like, while at the same time drawing up a protocol in which they specify the time, place and conditions under which they perform actions, and they document what content is visible when a specific URL is entered or a specific hyperlink is selected. Such an activity can also be treated as a procedural experiment specified in Article 211 of the Polish Code of Criminal Proceedings, constituting a kind of experiment to see what will happen when certain conditions arise. As far as evidentiary value is concerned, whether one treats the activity as an inspection or an experiment is secondary in this situation.

This action may seem archaic and superfluous to those unfamiliar with criminal proceedings, thus causing comments about “rewriting Internet” and the like. At the same time, however, in the authors’ opinion, the practice of protocol confirmation that a page contains certain content is generally correct and eliminates problems that may arise if such a procedural step as experimentation or inspection is omitted. One must also be mindful of the order under Article 207 of the Polish Code of Criminal Proceedings, which stipulates that if necessary, an inspection of the place, person or item shall be carried out.

Since inspection (or procedural experiment) is so important in the proceedings in question, the question arises – if it is omitted, can the proceedings continue? And consequently, if the content in question has been removed from the Internet before the judicial body drew up a report stating that it was posted on the site, will it be impossible to conduct proceedings on such a posting?

Obtaining information from site administrator

Depending on which website a certain content was posted on, it may be possible for the judicial body to request the site administrator to provide the exact content posted (article, post, comment, graphic, etc.), along with details of the user who posted it, such as their IP address, login, email address, etc. It would certainly be extremely difficult for the opposing party to challenge such information obtained from an independent entity, such as a site administrator. For a detailed discussion of the information that is obtainable depending on the platform on which the content is published, see The type and scope of data processed by online platforms, including “social media” providers.

Making a copy of the page

It seems that the creation of a mirror copy will present greater evidentiary value than, for example, saving a page as a PDF file, due to the fact that preserving the exact structure of the copied page in a mirror copy and downloading all its directories makes it easier to verify the authenticity of such a copy compared with a single file. Making a copy requires the use of software designed for this purpose, such as HTTrack Website Copier. It is worth pointing out that this action does not require any privileged access and is therefore not reserved for the judicial body, so it is worth creating a copy as early as at the stage of filing a criminal complaint.

Wayback Machine

One of the fascinating Internet resources that can be applied to criminal proceedings is the Wayback Machine digital archive run by the non-profit Internet Archive, available at archive.org. The idea behind this tool was to prevent the loss of content published on the Internet that cannot be accessed after a page is edited or closed. Its operation is based on web crawlers that regularly index publicly available content, thus archiving Internet resources. The archive.org service, however, gives you the option to designate the site for saving yourself (this functionality is available at <https://web.archive.org/save>). This way, the content will be protected from deletion, since there is very little possibility of challenging the credibility of the site version saved in this way – the authors are not aware of any cases where data obtained with the Wayback Machine has been challenged in criminal proceedings.

Notary certification of page content

One method of securing content posted on the web is to have a notary prepare a record of website opening. This is an official document, stating the exact content available at the time of its drafting, which should be considered a less questionable method than the notifier securing the content themselves. At the same time, however, this instrument is rarely used in criminal proceedings – it is more often used in civil proceedings.

6 Rules for formulating evidentiary motions

Introduction

In criminal proceedings, a lot of evidence is admitted *ex officio*²⁰. This means that the prosecutor, police officer, court or any other body conducting a particular proceeding at a particular stage independently decides to obtain the evidence in question.

This does not preclude the initiative of the parties to the proceedings, just the opposite in fact. The parties have the right to file a letter of request²¹, and the judicial body (court, prosecutor, police officer) is obliged to respond to such requests.

Who, in practice, can file an evidentiary motion? The Polish Code grants this right to the parties. At the pre-trial stage (i.e., before an indictment is filed in court, when an investigation or inquiry is underway), the following are considered parties: the victim and the suspect.²² At the stage of judicial proceedings (after the indictment is filed in court and before the final judgment is issued), the parties to the proceedings are the defendant, the prosecutor and the subsidiary prosecutor²³.

A social organization may, depending on the situation, have the status of an aggrieved party, in which case it is entitled to the rights of a party, including the right to file evidentiary motions.

20 According to the principle of *ex officio* action, as defined in Article 9 of the Code of Criminal Procedure (k.p.k.).

21 In accordance with Article 167 of the Code of Criminal Procedure.

22 In accordance with Article 299 § 1 of the Code of Criminal Procedure.

23 In accordance with Article 45 § 1, Article 55, and Article 367 of the Code of Criminal Procedure, the prosecutor acts before the court as the „public prosecutor.” However, in some cases, another authority may serve as the „public prosecutor,” such as the National Revenue Administration (in cases concerning tax crimes). Instead of the public prosecutor, a private prosecutor may appear (in cases prosecuted upon private accusation, such as defamation or insult), or an auxiliary prosecutor may intervene (in the situation of a case being dismissed twice or the prosecutor refusing to initiate proceedings twice).

To whom should an evidentiary motion be directed?

An evidentiary motion should be addressed to the authorities that are conducting the proceedings at a given stage.

In judicial proceedings, the court is such an authority.

What must an evidentiary motion contain?

An evidentiary motion cannot be written entirely freely. It should include the following:

1. the evidence to be conducted (mandatory);
2. the circumstances to be proven (mandatory; this is known as the “facta probanda”);
3. the manner in which the evidence is to be admitted (optional – not a must²⁴);
4. justification (optional – it is not necessary to include it, but it is desirable).²⁵

Example: I request to interrogate Jan Kowalski as a witness to prove what persons, during the period covering 12 November 2024, 4:45 PM, had access to the Internet connection provided by S.A. Internet Provider to Jan Kowalski at the address ul. Uliczna 1/1 in Warsaw. | Justification: on 12 November 2024, at 4:45 PM, an as yet undetermined user of the “X” portal published a post containing incitement to hatred based on racial differences, with the content “(...)”, from a user account named @Ogien123456789. In the course of the investigation, it was found that this user published the post using an IP address belonging to the network of S.A. Internet Provider, which provided Internet access service to Jan Kowalski at ul. Uliczna 1/1 in Warsaw. It was further established that the address is home to a co-working office run by Jan Kowalski, and that access to the Internet connection could be available to all people staying there. In order to verify the identity of the author of the aforementioned post, it is first necessary to establish the group of people who had access to Jan Kowalski’s Internet connection at the aforementioned office. Subsequently, it will be possible to identify the actual author of the post in question.

As can be seen in the example above – the evidentiary motion may seek to uncover other sources of evidence²⁶ that will only then lead to the clarification of circumstances relevant to the case

²⁴ In accordance with Article 169 of the Code of Criminal Procedure

²⁵ In a procedural document, the justification is included „as needed” – in accordance with Article 119 § 1 point 3 of the Code of Criminal Procedure. Including a justification with the evidence motion is appropriate. The justification can explain why presenting a specific piece of evidence in a given case is necessary and what information it may provide.

²⁶ The evidence motion may aim at detecting or assessing the proper evidence – Article 169 § 2 of the Code of Criminal Procedure.

(the authorship of the disputed post on the “X” portal). Attaching a justification to the motion is reasonable. If this justification had not been provided, it would have been “easier” for the judicial body to dismiss the evidentiary motion with the argument that Jan Kowalski runs an office to which many people have access, and therefore it is “impossible” to determine the author of the post. Explaining that the application seeks precisely to establish this group of people, which is a prerequisite for singling out the perpetrator of the crime further down the line, makes the prospect of the motion being dismissed less likely.

Formulation of facta probanda

It is important that facta probanda are formulated in a specific way. They should indicate the specific circumstances to be established by evidentiary proceedings.

It is not appropriate to stop at general statements such as:

Example (incorrect practice!): I request the admission of evidence (...) in reference to the case.

Example (incorrect practice!): I request the admission of evidence (...) in reference to the crime referred to in the complaint.

Example (incorrect practice!): I request the admission of evidence (...) in reference to the circumstances referred to in the complaint.

The correct practice is to formulate specific facta probanda, such as:

Example: I request to admit evidence (...) to prove what persons, during the period covering 12 November 2024, 4:45 PM, had access to the Internet connection provided by S.A. Internet Provider to Jan Kowalski at the address ul. Uliczna 1/1 in Warsaw.

Example: I request to apply to (...) to determine what IP address and network port number were used to publish a post with the content (...) dated 12 November 2024, at 4:45 PM on the account of user @Ogien123456789 on the “X” portal, and what the exact date and time of publication (with accuracy to the second) was.

Example: I request to apply to (...) to identify the customer (indicating name, surname and possibly name and full address and contact details) using IP address (...), network port number (...) on 12 November 2024, at 4:45:23 PM, provided by S.A. Internet Provider.

Incorrect or careless formulation of the facta probanda may lead to the dismissal of the evidentiary motion even if its consideration in a given case would be substantively justified.

How do law enforcement agencies handle an evidentiary motion?

If a prosecutor, police officer or court grants an evidentiary motion, they are not obligated to issue any formal ruling on the matter. The failure to issue any ruling in this case does not violate the rules of criminal procedure.

If the prosecutor, police officer or court dismisses the evidentiary motion, they issue a judgement.

Challenging the dismissal of the evidentiary motion

Judgment on dismissal of an evidentiary motion is not subject to appeal. The primary means of challenging the judicial body's decision is therefore unavailable in this case.

However, there are grounds for challenging the dismissal of an evidentiary motion in an appeal against a decision (unfavorable to the author of the motion) that would end the proceedings. Such means of appeal include: a complaint (against a decision to discontinue or refuse to initiate proceedings) or an appeal (against a court judgment).

Example: ABC Association is acting as an aggrieved party in the case. It directs an evidentiary motion to the prosecutor. The prosecutor issues a judgment dismissing this evidentiary motion on the grounds that it is clearly aimed at prolonging the proceedings. Subsequently, these proceedings are discontinued. In these circumstances, it is legitimate to raise the issue of the unjustified dismissal of the evidentiary motion in the complaint against the decision to discontinue the proceedings.

Authors:

Jakub Kłosiński – Prosecutor at the District Prosecutor’s Office for Warsaw-Praga, currently delegated to the Provincial Prosecutor’s Office in Warsaw (Economic Crime Division). He has handled investigations into the activities of transnational organized groups involved in vehicle and drug-related crime. Currently, he serves in the Cybercrime Division.

Jędrzej Kupczyński – PhD candidate at the Department of Criminalistics, Faculty of Law and Administration, University of Warsaw; prosecutor at the District Prosecutor’s Office for Warsaw-Wola in Warsaw. A graduate of the Faculty of Law and Administration at the University of Warsaw and the National School of Judiciary and Public Prosecution. His academic interests include criminalistics, particularly tool mark examination and issues related to lockpicking, burglary tactics, as well as new technologies in criminal law and forensic science. Professionally, he specializes in issues of cybercrime, investment, and stock market-related offenses. He is currently preparing a doctoral dissertation on the use of body-worn cameras (cameras mounted on uniforms) in police work and as evidence in criminal proceedings. A member of a research team conducting a project titled „Body-Worn Cameras in the Work of Law Enforcement and the Justice System.” On behalf of the Ministry of Justice, he is a member of the Polish-Norwegian bilateral working group on forensic experts. In his free time, he enjoys hiking in the mountains, cycling, scuba diving, and freediving.

Joanna Grabarczyk-Anders – is a social activist with approximately fifteen years of experience in the fields of hate speech, bias-motivated crimes, and online safety. She is a co-founder of the Hejtstop campaign and currently collaborates as an expert with the Jewish Association Czulent. Her expertise includes conducting research, analyses, and preparing reports on the scale of hate-motivated incidents, the use of hateful content in election campaigns, the removal of illegal content by IT services, and the phenomenon of disinformation in social media. She also specializes in issues related to underreporting within minority organizations. As a qualified trainer in the areas of online safety, hate speech, and hate crimes, she conducts training sessions for various professional groups, including police officers, lawyers, content moderators, and minority organizations. Her areas of interest also include the responsibility of network administrators for content, securing and collecting evidence, and identifying perpetrators of crimes. Since 2023, she has been a member of the Advisory Team to the Prosecutor General on combating hate speech and hate crimes.

JEWISH ASSOCIATION CZULENT

The Jewish Association Czulent is an independent, nonprofit organisation, both national and international in scope, primarily involved in advocacy work. Our platform brings together professionals from the Jewish community in Poland and beyond. Our advocacy work encompasses political, social, and legal dimensions, and is carried out by implementing innovative educational solutions and building coalitions for openness, against antisemitism, racism, and discrimination. We collaborate with institutions, public administration, and dialogue organisations to shape public attitudes and contribute to changes in Polish legislation regarding tolerance and the fight against racism.

Our partners include the OSCE Office for Democratic Institutions and Human Rights (ODIHR), the American Jewish Committee Central Europe, and the National Democratic Institute. Czulent undertakes comprehensive initiatives to counter antisemitism, which include analyses and reports on the phenomenon of antisemitism within the Visegrad Group countries, and is also involved in strategic litigation activities. We operate the zglosantysemityzm.pl platform, which facilitates the reporting of antisemitic incidents and crimes, and provides legal support to victims. Through international coalitions such as the European Network on Monitoring Antisemitism (ENMA), the Coalition to Counter Online Antisemitism (CCOA), the European Network Countering Antisemitism Through Education (ENCATE), and the European Network Against Racism (ENAR), we collect and promote best practices, and recommend solutions at the European level.

