TO DISCLOSE OR NOT TO DISCLOSE? – THAT IS THE QUESTION

by

SZYMON GOŁĘBIOWSKI*

An infringement of copyright entitles the right-holder to bring an action before the court against the infringer in order to seek damages. Although the personal data of the tortfeasor is also protected by law, the right-holder needs them in order to name the defendant and commence a lawsuit. What can be done if the controller of the data refuses to transfer them? In Promusicae *case, the ECJ left this question without an answer. The only guarantee constitutes a hint that an establishment of an obligation to disclose the personal data for the purposes of civil proceedings should be viewed from the perspective of inter alia ECHR, TRIPS and the e-commerce Directive. The Provincial Administrative Court in Warsaw delivered several judgements in similar cases and set forth that there is an obligation to disclose the personal data. Still, there is a loophole in Polish legislation. Perhaps the mentioned verdicts are going to influence the relevant legislation and legal practice. The crucial problem which courts and administrative bodies have to face is a balance which has to be struck between the right of access to the court and the right to protection of personal data. The purpose of this presentation shall be to critically analyse the Polish legislation and case-law concerning data protection and possibility of their disclosure for purposes of civil proceedings.*

KEYWORDS:

Data protection, IP address, disclosure, civil proceedings, Poland, defamation, Promusicae

* 5th year Master student, simmon@op.pl, University of Wrocław, Faculty of Law, Administration and Economics, www.prawo.uni.wroc.pl.

1. EUROPEAN STANDARD

The Promusicae case (2008) left within the recognition of the Member States the question of establishing or not *an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.* The only requirement is to *take care to rely on an interpretation of* [the EU directives] *which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order and also the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.*[1]

Leaving aside the circumstances of *Promusicae*, it must be born in mind that the problem in question concerns not only infringements of copyright but also defamation, libel and other torts which can be committed in the cyberspace and can be pursued in the course of civil proceedings. Such a vast area of application means that all the jurisdictions within the European Union are likely to be required to decide over similar cases. Although, pursuant to *Promusicae* judgement every Member State has a discretionary power to choose its own solution, there are some common questions which should be faced according to the uniform standards before all 27 jurisdictions. The following deliberations are aimed to give an insight into the Polish legislation and the case law concerning the problem.

2. PERSONAL DATA ON THE INTERNET

Every minute individual users transmit a plethora of information enabling to define their identity. These could be a name (e.g. in the social networks, like Facebook), a nickname (e.g. while signing an e-press article), an e-mail address (the content of the login could reveal some information, esp. when it consists of the name). These pieces of information do not always constitute personal data in the legal meaning and are mostly not sufficient to fulfill the requirements necessary to define a defendant for the purposes of civil proceedings or an accused for private criminal proceedings. In some circumstances the identity of the defendant can be determined easily (e.g.

[1] ECJ, Productores de Música de España (Promusicae) v Telefónica de España SAU, Case 275/06, [2008], ECR I-00271, par. 70.

attributing a postal address to an individual who has a MySpace profile). In any case, there are situations where a considerate workload is needed to find out the identity of an infringer. Data controllers are obviously reluctant to undertake such a challenging procedure as it undermines the trustworthiness towards them because particular users want to remain utterly anonymous.

3. DISPUTES OVER THE IP ADDRESS

The underlying question, strongly related to the issue of protection of personal data on the Internet is the essence of the IP address and its possible classification as a piece of personal data. Every computer or network connected to the Internet possesses a unique sequence of digits which enables to communicate with other users properly. This number called the IP address is usually automatically assigned to a user willing to connect to the web. The IP address could be altered easily for every new connection. However, most users explore the Internet using the same default number as there is no need to change it every time. To conclude, it is possible to identify a particular computer or network from which the data were transferred. That does not necessarily mean that when knowing the IP address we can define the identity of the infringer. After assigning the IP address to the device it can turn out that the computer is placed in the Internet café or university network and that it is no longer placed in the network area as it was a portable device (laptop or notebook). Such an IP address enables the identification of a natural person only as a part of a set of data available for the controller at the time of obtaining information, e.g. using the credit card simultaneously with a computer or being recorded by CCTV placed in an Internet café.[2] The IP address can be useful while defining a place but not always a natural person. Even if the infringer is finally identified in the course of a lengthy and expensive procedure, it can occur that he or she cannot be liable in tort (e.g. due to lack of active capacity).

Both the Directive 95/46/EC[3] and the Polish Act on the Protection of Personal Data[4] (hereinafter: DPA) stipulate that:

---

[2] Kowalczuk, I. 2010, Comparative questionnaire. Data protection [in:] Good Governance in the Public Sector, ed. E. Galewska, published individually, Wrocław, p.115-116.

[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ *L 281 , 23/11/1995)*

1. Within the meaning of the Act personal data shall mean any information relating to an identified or identifiable natural person.

2. An identifiable person is the one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

3. A piece of information shall not be regarded as identifying where the identification requires an unreasonable amount of time, cost and manpower [art. 6 of the DPA, see art. 2(a) of the Directive].

It is undeniable that in some circumstances the IP address enables to identify a particular device which obviously is used by a natural person. However, an aggrieved party willing to commence a lawsuit is unable to define the infringer when he or she possesses only the IP address. An intermediation of other entities is required, *inter alia* ISP. According to the Opinion 4/2007 of the Data Protection Working Party, *Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically "log" in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive…).*[5] The Working Party acknowledged that the IP address can constitute a personal data, esp. in cases when a copyright holder requires it to identify the infringers (like in *Promusicae*).

4. POLISH COURTS FACING THE PROBLEM

The first case in which Polish judicial authorities had to face the problem took place in 2004. The Provincial Administrative Court in Warsaw[6] had to decide over the disclosure of IP addresses to the prospective plaintiff who was offended by the users on a discussion forum. He initiated an action before the civil court and lodged a private indictment to the criminal division. Both the judicial institutions obliged the petitioner to complete the claim and the bill of indictment by determining the personal data of the

[4] Act of 29 August 1997 on the Protection of Personal Data (Ustawa o ochronie danych osobowych) – *Journal of Laws 1997, No 133, Vol. 883 with amendments (official translation).*

[5] Opinion 4/2007 on the concept of personal data, 20th June 2007, 01248/07/EN, WP 136.

[6] Judgement of 9 February 2005, doc.no. II SA/Wa 1085/04.

defendant/accused. The only traces left by the tortfeasors on the Internet were their IP addresses which were recorded automatically on the server but the Internet Service Provider was the sole entity that was able to attribute them to particular users. The ISP refused to transfer the desired addresses claiming that they did not constitute personal data. The applicant complained against the refusal to the Inspector General for the Personal Data Protection (hereinafter: GIODO) who ruled that the private entity who possessed IP addresses of the users was obliged as the controller of the data to disclose them to the applicant. According to the code of administrative procedure[7] the ISP submitted a motion for rehearing of the case but the Inspector General upheld the decision. Subsequently, the ISP appealed to the administrative court which annulled the attacked decision arguing that there was no obligation imposed on the private controllers to disclose the data. The basis of the verdict was the result of the wording of the Polish DPA rather than the unique nature of IP address. The provision of Art. 29(2) of the DPA constituting a legal basis for the disclosure of the personal data was applicable only to petitioners from the public sector, leaving private entities without the possibility to effectively demand the personal data (see: below, *Disclosure in Polish legilation*). The question of IPs, irrespective of the doctrinal discussions and Inspector's official statements in the matter, was not analysed deeply in the judgement but the administrative court pointed out that they can constitute personal data.

5. THE AMENDMENT AND ITS IMPACT

As a result of the criticism of the scholars the Polish DPA was amended on 22 January 2004[8] in the way that it embraced private petitioners as well. The first judgement concerning the Internet on the basis of the new provision was delivered in 2007.[9] The same court ruled that the data controller was obliged to disclose the personal data of the infringer if the applicant fulfilled all the preconditions defined in this article. This decision was given on the basis of the Press Law – not IPs but postal addresses were demanded by the a prospective plaintiff but as it was mentioned above, on the Internet there are stored many sorts of information which enable to define the identity of a natural person. The petitioner, J.K. requested from the press editor who was

[7] Act of 14 June 1960 – Code of Administrative Procedure (Kodeks postępowania administracyjnego) – *uniform text – Journal of Laws 2000, No 98, Vol. 1071 with amendments.*

[8] Journal of Laws 2004, No 33, Vol. 285.

[9] Judgement of 5 October 2007, doc.no. II SA/Wa 975/07.

the controller of the data pursuant to the legislation, the postal addresses of two journalists he wanted to sue for violation of personal interests committed in the article published on the Internet. According to the case law of administrative courts, the written materials published in the Internet constitute a press within the meaning of Polish law. The editor refused to communicate the addresses required by civil court, therefore the applicant filed an appeal with the Inspector General. The GIODO acknowledged the existence of such a right after the amendment of the DPA and obliged the press editor to disclose the data. The controller lodged a complaint to the administrative court who upheld the position of the Inspector General. The constitutional right to sue prevailed over another fundamental right – the right to protection of personal data. This interpretation was in accordance with an established case law of the administrative courts concerning the press law but this time it was the first verdict concerning the Internet press and the personal data placed therein.

6. CELEBRITY STRIKES BACK

The most recent case where the legal status of IP addresses was on stake took place in 2010 before the same court and is still not final.[10] Two users wrote offensive statements constituting a defamation (according to the Polish civil code of 1964 – a violation of personal interests) of a famous singer, Maryla Rodowicz. The celebrity decided to initiate civil proceedings against the infringers but the court required to determine the personal data of the defendants. The plaintiff claimed the possession of the IP addresses of the users from the discussion forum administrators. They refused to disclose the identities, claiming that they do not constitute personal data according to the terms of the DPA. The Inspector General demanded the controller to disclose them but the ISP appealed to the court. This time the very nature of IP address was taken into consideration. The company who possessed the information about IP addresses of the users claimed that IP does not constitute the personal data in the meaning of 1997 Act as it is only *a piece of information about the number of an interface or a network by which the communication took place.* The court refused to accept such an argumentation as it invoked the abovementioned Opinion of the Working Party and ruled that the identity of the natural person could be defined even by the reference to the identity of the material objects he or she used.

[10] Judgement of 3 February 20010, doc.no. II SA/Wa 1598/09.

The Court justified its decision by placing the following statement in the judgement:

It needs to be emphasized that so-called "network excesses" more and more often violate personal interests of other persons. It is too easy for theoretically anonymous persons to express their opinions on Internet forums and harm others.

The Court takes the position that the right to free and anonymous opinion cannot protect persons who violate other persons' rights from the liability for expressed statements. On the Internet nobody is and can be anonymous. In fact, the process of establishment of the natural person's identity can be hampered, however considering the fact that every computer leaves a trace in the Internet – an IP address whereby it is possible to define the computer from which the statement was posted – it enables to identify indirectly the identity of a person who posted a statement.

As it can be seen, the reasons for the sentence are not supported with typical legal argumentation but the judicial panel relied on criteria of justice. The court felt obliged to correct the mistakes of the lawmaker because there were not many legal remedies which make possible punishing the authors of the offensive forum posts. Arguing that the Internet became a field of many infringements and that the obligation of ISPs to disclose IP addresses could be an effective remedy for the prospective plaintiffs in outfighting the "network excesses", the court obliged the controller to communicate the IPs of the tortfeasors. Although the intents of the court are justified, it appears that the judicial panel exceeded its powers by attempting to regulate over the issue. The boundaries of the teleological interpretation seem to have been surpassed and the argumentation of the court constituted *contra legem* interpretation. It must be borne in mind that the literal meaning of the DPA may be controversial but it is the lawmaker who should decide over establishment or not of an obligation, not the judicial body. The sole existence of the problem of anonymous offenders and a misty possibility of determining their identity should be resolved on the level of an official enactment. The court could point out the mistakes of the lawmaker, like in the first of abovementioned judgements. Moreover, the solution adapted by the court imposes expensive obligations on ISP connected with attributing the number to a particular user. The judgement is still not final and the Supreme Administrative Court is dealing with it at the moment.

7. DISCLOSURE IN POLISH LEGISLATION

The legal basis for disclosure of the personal data has been the provision of the article 29 of DPA which states:

1. In case of providing the access to the data for the purposes other than including into the data filing system, the controller shall disclose the data kept in the data filing system to persons or subjects authorised by the law.

2. Personal data, exclusive of data referred to in Article 27 paragraph 1 [so-called "sensitive data"], may also be disclosed, for the purposes other than including into the data filing system, to persons and subjects other than those referred to in paragraph 1 above, provided that such persons or subjects present reliably their reasons for being granted the access to the data and that granting such access will not violate the rights and freedoms of the data subjects.

(…)

The wording of the cited provision (esp. the expression "may" in the section 2 thereof) raised many controversies as it was unclear whether it established the right of the aggrieved party to effectively demand the communication of personal data of the infringer and the corresponding obligation of the controller to disclose them. The contrary interpretation of the article in question was that it granted the right to the controller to decide by his or her own will over the disclosure of the data what would be in accordance with his or her interest and strengthen the trustworthiness of the users towards him or her. The second interpretation was in accordance with the literal meaning of the DPA as in the article 29(1) we have an expressed obligation imposed on the controllers (*the controller shall disclose*). In the following section there is an expression indicating the existence of right, not obligation (*personal data (…) may (…) be disclosed*). Such a wording of an enactment caused many problems and the wording of said article needs to be amended.

Before the amendment of 22 January 2004 the invoked stipulation concerned only controllers of the data from the public sector. This raised many doubts whether such a disclosure should be performed in the form of administrative decision or not.[11] Such was a legal situation of the circumstances in the first of abovementioned cases. To summarize, the private controller was not obliged to disclose the personal data but in the first judgement the court pointed out the existence of the perilous loophole

[11] Barta, J., Figajewski, P. & Markiewicz, R. 2004, Ochrona danych osobowych. Komentarz, Wolters Kluwer, Warsaw, p. 605-610.

in the DPA which granted for private controllers a dangerous discretionary power in freely deciding over disclosure of such data. The 2004 amendment was intended to fill the gap and embrace all the categories of controllers (irrespective of the sector they belong to) by an equal obligation.

What is worth noticing is the fact that the Art. 29 of the DPA was abrogated by the amendment of 29 October 2010[12] and is no longer in force from 7 March 2011. Now, the legal basis for the disclosure of IP addresses could be only the Art. 23(1) governing the general rules of processing the personal data. This stipulates as follows:

The processing of data is permitted only if:

(...)

2) processing is necessary for the purpose of exercise of rights and duties resulting from a legal provision,

(...)

According to the Art. 7(2), processing of data shall mean any operation which is performed upon personal data, such as collection, recording, storage, organization, alteration, **disclosure** [*emphasis added*] and erasure, and in particular those performed in the computer systems.

It transpires from the cited provision that the disclosure of data as a part of processing thereof is permissible for the purpose of exercise of rights resulting from a legal provision (i.e. commencing a lawsuit before the civil court).

Untill the recent amendment the Art. 29 was considered to be a *lex speciali* in relation to the Art. 23 and such was the reasoning of the Court in the first case (from 2004) what resulted in refusal to disclose the IP addresses for private petitioner. It seems that the abrogation of the controversial provision from the DPA was a good solution an is likely to eliminate possible disambiguations in the future (such was also the intent of the authors of the amendment).[13] Such a decision of the Parliament was probably influenced by the abovementioned controversies as well. All, in all the case-law invoked concerning the disclosure of IP address and its affiliation the personal data is still likely to be followed by other judicial authorities and is a milestone in shaping Polish *Promusicae* standard.

---

[12] Act of 29 October 2010 on the Amendment of the Act on the Protection of Personal Data and some other acts (Journal of Laws 2010, No 229 item 1497).

[13] Parliamentary bill (Druk sejmowy) No 488 of 21 December 2007, p. 4 (available at: http://orka.sejm.gov.pl/Druki6ka.nsf, Polish version only).

8. CONCLUDING REMARKS

The two judgements (from 2007 and 2010) were delivered on the basis of the amended provision of the article 29(2) of DPA. As it was mentioned, the outcome of these sets of proceedings was utterly different in comparison to the first case. In 2007 and 2010 the Provincial Administrative Court ruled contrary to the literal meaning of the stipulation. The constitutional and conventional right to sue prevailed over the right to privacy and to protection of personal data. Such a solution may constitute a contradiction to the direct wording of Polish DPA but is definitively in accordance with the system of values adopted by the Polish lawmakers.

It must be borne in mind that it seems the Polish authorities have adopted their own solution over the discretion pointed out in *Promusicae*. However, the cases invoked concern only forum libels and press defamations committed in the cyberspace, so many other infringements, e.g. peer-to-peer file sharing still await their "precedent" decisions. Moreover, all these cases were ruled over by the provincial administrative court (in fact, it was the same court every time due to territorial jurisdiction over the Inspector General who is situated in Warsaw) which is a judicial body of the first instance so the stance of the Supreme Administrative Court, the Supreme Court or the Constitutional Tribunal is still not determined. In addition, the most recent judgement being the most controversial one is still not final and one of the parties has lodged a cassation appeal. The justification of the court in the last case revokes some extra-legal values and constitutes an attempt to lay down the new regulations by the judicial panel regardless of the lack of legal basis for such a step. The purpose of such a resolution seems to be justifiable but the width of the problem indicates that particular judgements are not able to deal with it. The new justification should be adopted – the leeway left by the ECJ in *Promusicae* is too vast to be filled by a judicial authority in the country of statutory law culture. This part of the judgement shows the helplessness of the public authorities in the face of the Internet.

It seems also that the new reality created with the spread of the Internet exposes many drawbacks of the traditional civil proceedings. The Roman model of civil procedure as the litigation between the two entities where both parties of the dispute are required to be defined precisely seems to be out of date. On the other hand, any attempt to strengthen the control over the Internet, e.g. establishment of an obligation to reveal one's personal data

before logging in to the server, restricting the liability of ISPs or webmasters constitutes violation of the constitutional and conventional right to privacy and is unacceptable in the democratic society. The essence of the Internet and the electronic communication makes these fields very sensitive on every legislative innovation. Perhaps, the Internet where the freedom of speech is abused frequently is a price we have to pay for the democracy. In any case, the whole process of demanding the IP addresses, determining the identity of the user, demanding the administrative body to enforce the controller to communicate the data and finally commencing a lawsuit which can occur failed makes the whole effort expensive, burdensome and doubtful and in the result the infringements committed on the Internet remain often unpunished.