Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Recommendation of the FDPIC regarding the processing and transfer of electronic data traces by a Swiss company acting on behalf of copyright holders

Initial situation

A Swiss company (which will be referred to as Company X), acting on behalf of the media industry, has been engaged in trawling so-called peer-to-peer networks with a view to uncovering copyright infringement resulting from the illegal sharing of music and video content on the Internet. In order to do so, it has developed special software which allows it to automatically track copyrighted material being offered for illegal download in various P2P networks. The software tries to download the content, and as it does so, it records the data traces generated during the Internet connection by the supplier of copyrighted works. The data, which are collected without the knowledge or involvement of the person concerned (including the bona fide owner of the Internet access), are then periodically transferred to the rightsholders of the relevant work or their legal representatives abroad.

As a rule, the connection data alone (in particular the IP address) do not enable the direct identification of the person who is using the Internet access, be it the Internet account owner or the copyright infringer. The identification data assigned to the IP address (such as name, address, etc.) are only accessible to the Internet service provider (ISP), and are protected by secrecy of telecommunication regulations. Secrecy of telecommunications may only be lifted in the context of criminal proceedings by the investigating authority for the purpose of discovering the Internet account owner's identity. It is for this reason that copyright holders or their legal representatives, having obtained the connection data from Company X, initiate criminal proceedings against persons unknown. As this automatically gives them right of access to the files, they are able to find out the name and address of the Internet account owner. Armed with this information, they then claim damages from the Internet account owner (who may not necessarily be the copyright infringer) and demand the signing of a cease-and-desist letter.

As Internet connection data (specifically IP addresses) are personal data, the processing operations that are being carried out in the present case clearly fall under the Federal Data Protection Act (FDPA). The methods employed by Company X for this purpose may infringe the privacy rights of a large number of persons, particularly as the data are processed without the knowledge of the persons concerned. It is for this reason that the Federal Data Protection and Information Commissioner (FDPIC), invoking Article 29 of the FDPA, undertook a closer inspection of the facts.

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

Examination of the Legality of the Data Processing

In order to determine whether the data processing has been conducted in conformity with the FDPA, it is necessary to ascertain whether or not data protection principles have been respected. The principles in question are: the principle of legality (Article 4, paragraph 1 FDPA), the principle of purpose (Article 4, paragraph 3 FDPA), the principles of good faith and transparency (Article 4, paragraph 2 FDPA), the principle of proportionality (Article 4 paragraph 2), as well as the principles relating to the transfer of data abroad (Article 6 FDPA). In cases where these principles are not respected and the processing of data is deemed to have infringed an individual's privacy rights (Article 12 FDPA), it is necessary to verify if there are any grounds that might nevertheless justify such processing (Article 13 FDPA).

Data protection principles

Article 4, paragraph 1 of the FDPA states that personal data may only be collected by lawful means. Participants in peer-to-peer networks voluntarily make works available to be shared by others. During this process, connection data are exchanged between the programmes that provide access to such networks. To date, there is no specific legal basis in Switzerland which allows the systematic recording of IP addresses in P2P networks. By the same token, however, systematic data collection is not expressly forbidden either. As Company X automatically and proactively collects data without the knowledge of the persons concerned, and since the data can be used as a basis for instituting criminal proceedings, the FDPIC is of the opinion that data processing under such circumstances needs to be explicitly covered by a legal basis. The law should also determine the evidential value of the data collected on the Internet by private individuals (in this case Company X) as well as their admissibility as a means of proof. Other countries are also currently discussing the possibility of adopting the appropriate regulations.

According to Article 4, paragraph 3 FDPA, personal data may only be collected for the purpose originally indicated, or as provided by law, or as warranted by circumstances. In a P2P network, connection data are made accessible for the purpose of sharing content. The systematic collection and storage of such data as a means of tracking copyright violations does not conform to the original purpose. The change of purpose is not covered by any existing law, nor is it discernable to the normal users of the software (or to the Internet account owner). Thus, Company X has failed to comply with the purpose principle.

Article 4, paragraph 2 FDPA refers to the principle of good faith, which in turn forms the basis of the principle of transparency, according to which the individual must be made aware that data processing concerning them is being carried out. In other words, the person concerned must either be informed, or must expect, the data to be processed in the light of the circumstances. In this particular case, Company X collects data without the knowledge of the person concerned (who may be the Internet access owner or the actual copyright infringer), and therefore this must be deemed to be covert data acquisition. As the connection data generated by the file-sharing software programmes are exchanged in principle without the user's knowledge, and as Company X has developed its own special programme allowing it to access and record the data, users of the software (i.e. copyright infringers) cannot expect their data to be processed. The Internet account owner (unless he is also the copyright infringer) is not directly involved in the exchange of content, and therefore can never be informed that

his data is being processed in such manner. Hence, Company X has infringed the transparency principle.

Company X also collects data with a view to identifying the Internet account owner and using that information to press claims in the civil courts. Under current law, the identification of the Internet account owner may only be disclosed within the context of criminal proceedings, as the lifting of telecommunications secrecy is conditional upon this. Only in such circumstances can ISPs (internet service providers), who alone can identify the account owner on the basis of connection data, be required to hand the information over. When copyright holders or their legal representatives initiate criminal proceedings with a view to ascertaining the identity of an Internet account owner in order to then sue for damages, they are circumventing the secrecy of telecommunications. This may be considered an abuse of law, particularly as the legal principle that enshrines the right of access to records within the context of criminal proceedings against a copyright infringer is used to claim damages against a possibly bona fide Internet account owner. Furthermore, the copyright holders or their legal representatives do not usually wait for the criminal court to hand down its sentence before they sue for damages in the civil courts, even though the Internet account owner may not be guilty of infringing copyright. The abuse of the right of access to records within the context of criminal proceedings in order to sue the bona fide owner of an Internet access for damages, constitutes a breach of good faith. As this cannot be justified, there is no need to apply the proportionality test. If the secrecy of telecommunications is to be lifted within the context of a civil suit, the FDPIC is of the opinion that this must be covered by a legal basis in which the exact conditions under which such action can be authorised are set out. This is precisely what was done in the Federal Mail and Telecommunications Monitoring Act which can be invoked in criminal proceedings.

In the light of the above, conformity of the data processing carried out by Company X with the proportionality principle shall only be examined within the context of criminal proceedings. Data processing may be deemed proportional, if it is both suitable and necessary for achieving the required objective, and if the measures are considered reasonable and proportionate in view of the encroachment on an individual's privacy. The data processing carried out by Company X is suitable for narrowing down the circle of potential offenders and determining the exact circumstances of a copyright infringement, thereby creating a basis for the filing of charges that have a good chance of being upheld in court. Furthermore, this measure is necessary in order to obtain specific evidence and proof of the existence of a copyright infringement. As a basic principle, we consider that it is reasonable to expect the bona fide Internet access owner to submit to a criminal investigation as long as this does not cause him undue hardship. Such hardship does, however, arise when the copyright holder or their legal representatives are granted access to the files, and by these means are able to discover his identity and present him with large claims for damages. Rights holders can exercise their right of participation and control within the context of criminal proceedings without having to know the identity of an Internet account owner who is not guilty of any copyright infringement. Moreover, it is important to remember that there is nothing to stop them from claiming damages by bringing a civil case within the criminal prosecution. Only under such circumstances would the data processing undertaken by Company X be considered proportionate.

Company X, in processing the data, has failed to respect the principles of purpose and transparency, and has thus laid itself open to the charge of infringement of privacy as defined in Article 12 FDPA, and therefore, according to Article 13 FDPA, a justification must be provided. As the processing of the

data and the subsequent pressing of criminal charges used in order to sue for damages violates the principle of good faith and must therefore be considered an abuse of law, there can be no justification.

Justification

According to Article 13, paragraph 1 of the FDPA, the infringement of privacy is not unlawful if the injured party gives his consent, if there is an overriding private or public interest, or if it is justified by the law. As the data are processed without the knowledge of the person concerned, it cannot be argued that the data subject has given his consent. In the present case, no overriding public interest or legal basis can be invoked to justify the infringement of privacy.

For the data processing carried out by Company X to be considered lawful, it is necessary to prove an overriding private interest. That interest can only be found in the criminal charges filed for copyright infringement, while the abuse of process upon which the civil proceedings is based constitute a breach of the duty to act in good faith. There is a conflict of interests: on the one hand, the rights holders are entitled to press charges against individuals who infringe their rights and to demand damages; on the other hand, those same individuals are entitled to the protection of their privacy and informational self-determination (in particular bona fide Internet account owners). Company X has not used the right of access to the files granted by the investigating authorities solely in support of the criminal case it brings before the courts against copyright infringers. On the contrary, the information it obtains in this manner is used abusively in order to file civil claims against bona fide Internet account owners. By doing so, Company X undermines the secrecy of telecommunications which is protected under civil law, a practice which is widely used by the copyright holders. As the privacy rights of an unlimited number of bona fide Internet account owners are violated in the process, the fact of filing a criminal complaint cannot be considered as a sufficient ground as long as there is no guarantee that the identity of bona fide Internet access owners are protected in the context of criminal proceedings.

Conclusions and recommendation

The FDPIC notes that the data processing carried out by Company X infringes the principles of the Federal Data Protection Act, and that there are insufficient grounds to legitimise such an action. All the more so, because the rights holders abuse the right of access to the files in order to circumvent the civil law principle of the secrecy of telecommunications. At the time of the parliamentary debate on Article 51 of the Swiss Copyright Act, the legislator came to the conclusion that ISPs cannot legally be forced to provide information concerning the identity of the user of the Internet connection for the purpose of civil claims, and therefore considered that any legal action could only be pursued under private law. Furthermore, during the recent parliamentary debate on the transposition of the WIPO agreement, no such possibility was foreseen. The FDPIC therefore maintains that any lifting of the secrecy of telecommunications for civil law purposes requires a legal basis.

For these reasons, the Federal Data Protection and Information Commissioner has issued a recommendation that Company X immediately desists from any further data processing until a sufficient legal basis for a civil law use of the data has been established.

The company has 30 days after receiving the recommendation to inform the FDPIC whether it intends to comply or not. If the recommendation is rejected or ignored, the FDPIC can refer the matter to the Federal Administrative Court in accordance with Article 29, paragraph 4 of the Federal Data Protection Act.