datACT – Conference on data protection and trafficking

Where do all the data go?

European data protection law and the protection of personal data of trafficked persons

Marjan Wijers, Berlin 25 September 2013

Introduction

Over the last years there is an increasing focus on the collection of personal data of victims of trafficking. Personal data of trafficked persons are not only collected and exchanged in the context of criminal investigations and prosecution or the organization of national and transnational assistance, but also for all other kinds of reasons by national governments, intergovernmental organisations, NGOs and private businesses.

An example of State led collection of data are the National Rapporteur mechanisms in Europe. Some are based on the collection of non-personal, anonymous data about victims of trafficking, others, however, focus on the collection of personalised data of victims. An example of a private business is the Polaris project, led by a US based private enterprise, aiming at conducting analyses of trafficking trends.[1] The latter shows that data of trafficked persons increasingly also represent a commercial value.

Risks attached to data collection

A serious concern therefore are the privacy and safety risks attached to the collection, exchange and other forms of processing of personal data of victims. The protection of victims' private life and identity is not only crucial in light of their physical safety given the risk of retaliation from the side of their exploiters, but also in view of the risk of stigmatization and their chances to rebuild their life in the country of origin or destination. Moreover, victims of trafficking in the sex industry not only face the risk of reprisals on the part of the traffickers but also on the part of the authorities. In many, in particular Eastern European, countries prostitutes themselves are criminalized, thus exposing trafficking victims to the risk of arrest, prosecution and/or punishment. In this regard we should also not forget the reports of officials being involved in trafficking with the attached risk of abuse of data, not only by criminals but also by corrupt officials. Finally, it is crucial for victim's access to assistance that they can trust that their information is kept fully confidential by assistance providers.

Despite the fact that the risks are evident, it seems that the eagerness to collect data of victims overrides privacy and safety concerns. In practice this means that in the name of combating trafficking, rather than being protected, victims are exposed to extra risks. Although various anti-trafficking documents mention that data collection should be in line with data protection laws, there seems to be little awareness and knowledge of what this

[1] Named after the North star that guided slaves towards freedom along the underground railway. The project aims (among others) at conducting analyses of trends in human trafficking and publishing anonymous data regarding human trafficker activities, including, for example, "heat maps" showing concentrations and trends relating to trafficker activity.

implies and a surprising lack of guidelines on the conditions under which the processing of personal data of trafficked persons is lawful, its limitations and risks, and the protections which should be in place.

This brings us to the question of data protection instruments and what protection they offer.

Main instruments

The basis for all European data protection instruments is **Article 8 of the 1950 European Convention on Human Rights** (ECHR): the right to respect for private and family life, which prevents the public authorities from interfering with the private life of citizens unless certain conditions have been met. Similarly, the protection of personal data is considered an autonomous fundamental right in the EU Charter of Fundamental Rights (2009).

The two main instruments in the area of data protection are:

1. The so-called **Data Protection Directive**[2], which is the centre piece of legislation on data protection in Community law. The definitions and principles of the Directive are the main reference of data protection provisions of other instruments. All EU countries had to implement this Directive in their national legislation. It, however, excludes data processing activities in the area of police and judicial cooperation in criminal matters.
2. Given the limitation in scope of the Directive the 1981 **Council of Europe Convention 108** was the main reference in the fields of police and judicial cooperation till 2008, when a separate Framework Decision (2008/977/HA) in this area was adopted. The latter, however, only covers cross border data processing. For the processing of domestic data in criminal matters the convention is still the main instrument. Furthermore, the Convention covers more countries than the EU Data Protection Directive, as it is a Council of Europe Convention.

Main concepts

The two key concepts in both instruments are “personal data” and “processing of personal data”, which are both broadly defined.

- '**personal data**' means any information relating to an identified or identifiable individual. Data is considered personal when it enables anyone to link information to a specific person, even if the person or body holding that data cannot make that link. That means any information that identifies or can lead to the identification of one person (data subject) from the rest of persons falls under personal data.
- '**processing of personal data**' ('processing') means any operation which is performed upon personal data, including collection, recording, storage, retrieval, consultation, use, transmission, dissemination or otherwise making available, blocking, erasure or destruction.

[2] In full: *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.*

Basic principles

The **purpose of data protection** is to protect the individual about whom data are processed. This is achieved through a combination of rights for the individual (called "data subject" in data protection language) and obligations for those who process data (the "data processor") or exercise control over such processing (the "data controller").

The Directive, in short, defines the **conditions under which personal data may be processed**. It requires that each Member State implements these provisions in its national laws. It also required States to establish a national supervising body (NRA's: national data protection authorities). The Directive applies to both public and private sectors, like NGOs, IGOs and businesses, including international businesses whenever the controller uses equipment located within the EU to process data.

The Directive is based on **7 principles**:

Principles on Data protection

- **Purpose**: data should only be used only for the purposes stated and not for any other purposes
- **Consent**: personal data should not be disclosed or shared with third parties without the data subject's consent
- **Security**: collected data should be kept safe and secure from potential abuse, theft or loss
- **Notice**: data subjects should be informed as to who is collecting their data
- **Disclosure**: subjects whose personal data is being collected should be informed as to the part or parties collecting such data.
- **Access**: data subjects should be allowed to access their data and to correct any inaccurate data
- **Accountability**: data subjects should be able to hold data collectors accountable for following the above principles

Consent

A key concept is consent, which is defined as "any freely given specific and informed indication". More specific free consent can be defined as

"*a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other*."[3]

The latter description was specifically considered in the context of consent given under the threat of non-treatment or lower quality treatment in a medical situation, which as such cannot be considered as 'free'. This could very well extend to other forms of assistance services, such as psychological, social or legal assistance. When, for example, trafficked persons have to consent to the exchange of their personal data with third parties in order to get access to assistance services, this cannot be considered as freely given consent.

[3] Article 29 Working Party "Opinion on the definition of consent", p. 13

Sensitive data

Particularly interesting from the perspective of trafficked persons is the special category of 'sensitive data'. Both Convention 108 and the Data Protection Directive are based on the premise that certain categories of personal data present a greater risk to a person's private life than 'regular' personal data and therefore require extra protection. Processing of this data is subject to more stringent restrictions. This special category of data is also known as 'sensitive data'. Article 8(1) defines them as:

> "*data revealing racial or **ethnic origin**, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning **health or sex life**.*"

As a general rule the processing of sensitive data is prohibited, with limited exceptions under certain conditions and safeguards (art. 8 Dir). Exceptions are e.g. medical reasons, or the processing of data of its members by an association or trade union.

If none of the listed exceptions apply and the person concerned has not given his or her freely given, specific and informed consent, an exception on the prohibition of processing sensitive data is only justified when it has a legal basis, is necessary for reasons of substantial public interest, and is subject to suitable safeguards.

The interesting question is, of course, whether data on trafficked persons fall within this category 'sensitive data'.

This is especially important given the aforementioned increasing focus on data collection not only of offenders but also of (alleged) victims. Moreover, in the course of harmonizing data collection procedures in the EU and the OSCE region, streamlining cross-border assistance of trafficked persons, the development of transnational referral mechanisms and increasing cross-border police cooperation, personal data of trafficked persons is stored by a range of both governmental, intergovernmental and non-governmental organizations.

In many cases this regards sensitive personal data which may expose the trafficked person to the risk of retaliation from the part of the offenders, prosecution or punishment from the part of the authorities in countries where prostitutes are criminalized and social exclusion from the part of their social environment.

This makes the question whether or not data on trafficked persons should be qualified as sensitive data a highly relevant one.

It is obvious that "data concerning a person's sex life" may very well be applicable to data on persons trafficked for the sex industry, and to sex workers in general. This raises the question what must be understood under "sex life" in the sense of Article 8(1) Data Protection Directive.

The case of the Netherlands

I like to explain this at the hand of the example of the Netherlands.

In 2009, a Bill, aiming to combat trafficking, was submitted to Parliament which introduced mandatory registration of sex workers and the criminalisation of unregistered sex workers and their clients.

It was argued that mandatory registration would help to combat trafficking as it would provide insight in who were prostitutes and where they worked. Moreover, registration would provide an opportunity to have a "contact moment" with sex workers, so that victims could be identified and sex workers could be educated about their rights and possibilities for help.

As you might imagine, there were many reasons why the bill met massive resistance not only from sex workers, but from almost everybody working in this field. Not only did hardly anybody believe mandatory registration would help to combat trafficking, it was also obvious that a national register of sex workers is extremely privacy sensitive.

This raised the question whether mandatory registration of sex workers would fall under the prohibition on the processing of data concerning someone's sex life.

Initially, the Dutch Minister of Justice argued that the prohibition was not applicable since sex work should be regarded as work, implying that data on the fact that a person works in prostitution could not be considered as data on someone's 'sex life', as it referred to the person's professional life and not to his or her private sexual preference or sexual orientation.

That made it important how the concept of 'sex life' was defined and whether making a distinction between a person's private and professional sex life was justified.

'Sex life' is not defined or explained in the Data Protection Directive or its preamble. Neither does the jurisprudence of the EU Court of Justice provide for the interpretation of the concept of 'sex life'.

The case law of the European Court of Human Rights (ECrtHR), however, does provide some guidelines. The Court has judged in several cases that sexuality is part of the most intimate aspects of someone's privacy, which means that in a democratic society only especially serious reasons can justify interference of the government.

Moreover, the distinction between a person's professional and private life is not supported by jurisprudence of both the EU Court of Justice and the European Court of Human Rights (ECrtHR). In this respect the EU Court of Justice refers to the ECrtHR which in several cases has held that:

"the term 'private life' should not be interpreted restrictively" and that *'there is no reason of principle to justify excluding activities of a professional nature from the notion of "private life"'.*[4]

[4] ECrtHR, C-92/09 and C93/09 of 9.11.2010 (*Schecke & Eifert*), § 59; see also *Österreichischer Rundfunk and Others*, §§ 73 and 74; and ECrtHR 16 December 1992, Application No. 13710/88, *Niemitz v. Germany*, §29.

In one of its judgments the ECrtHR considered e.g.:

"There appears (…) to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature (…) This view is supported by the fact that (…) it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. Thus, especially in the case of a person exercising a liberal profession, his work in that context may form part and parcel of his life to such a degree that it becomes impossible to know in what capacity he is acting at a given moment of time.

To deny the protection of Article 8 on the ground that the measure complained of related only to professional activities (…) could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non-professional activities were so intermingled that there was no means of distinguishing between them."[5]

It was clear therefore that the distinction the Minister made between one's professional and personal sexual life could not stand the test of both the EU Court of Justice and the ECrtHR.

This forced the Minister of Justice to admit that the distinction between the professional and private life of sex workers could not be maintained, and that - contrary to his previous statement - registration of sex workers indeed concerned the processing of sensitive data.[6]

This implied that registration of sex workers was prohibited under article 16 of the Dutch Personal Data Protection Act (Wbp), which is the national transposition of the Directive. The next question was whether the conditions to make an exception on this prohibition were fulfilled.

According to article 8 Directive (and Art. 23 Wbp) an exception on the general prohibition to process sensitive data is only justified under strict conditions. It must be:

- necessary for reasons of substantial public interest
- subject to the provision of suitable safeguards, and
- have a legal basis.[7]

Whether the processing of sensitive data is justified by reasons of substantial public interest will have to be reviewed on a case-by-case basis. Criteria for this assessment can be deduced from Article 8(2) ECHR and the related jurisprudence from the ECrtHR:[8]

- It must serve a legitimate aim;

[5] ECrtHR 16 December 1992, Application No. 13710/88, *Niemitz v. Germany*, §29.

[6] See also: ECrtHR of 18 October 2011, Application No 16188/07, *Khelili v. Switzerland*, § 56 (only available in French): *"La Cour estime qu'en l'occurrence la mémorisation de données relatives à la vie privée de la requérante, dont fait partie la profession, et leur conservation, constituent une ingérence au sens de l'article 8 de la Convention, car il s'agit d'une donnée à caractère personnel se rapportant à un individu identifié ou identifiable. A cet égard, elle observe que, s'agissant de la profession de la requérante, la mention « prostituée » a été biffée du système informatique de la police et remplacée par « couturière ». Toutefois, il découle des arrêts des instances judiciaires du canton de Genève que la mention litigieuse jointe aux diverses affaires pénales n'a pas été supprimée."*

[7] Either by national law or by decision of the supervisory authority.

[8] See e.g. ECrtHR, 4 December 2008, Application No 30562/04 and 30566/04, *S. and Marper v. United Kingdom*. ECrtHR 18 May 2010, Application No 26839/05, *Kennedy v. United Kingdom*.

- The means must be proportional to the aim (principle of proportionality);
- There must be no other less severe/invasive means to achieve the aim (principle of subsidiarity).

To assess whether an exception could be legitimised by “reasons of substantial public interest”, we had to look at the aims of the Bill. Despite the rhetoric about combating trafficking, the aim of the Bill, in the end, boiled down to “to regulate prostitution and sex businesses” and “to facilitate supervision and enforcement”. A goal of which it is highly doubtful whether it justifies a serious violation of the privacy of all sex workers in the Netherlands, and which brings us to the question of proportionality. In addition, there are other, more effective means possible which constitute a less invasive violation of the privacy of sex workers. For instance, to intensify supervision of sex businesses instead of individual workers and to expand fieldwork to establish contacts with sex workers to provide them with information and assistance. This made it highly probable that the Bill would not stand the above test.

Next to the condition of a substantial public interest, suitable safeguards should be provided, in which the Bill did not foresee. Also, the question whether a safeguard is ‘suitable’ will be variable over time, especially in the light of technological developments. In the case of processing sensitive data the ECrtHR sets higher standards in regard to the security level, duration of data retention, access and (legal) safeguards provided for by law for the protection of privacy.

Beginning this year, following serious objections of the first Chamber of Parliament (Senate) against the mandatory registration of sex workers, the Minister was forced to withdraw the Bill.

Conclusion

It may be concluded that at least data on trafficked persons’ involvement in prostitution should be qualified as “sensitive data”. This implies that strict conditions on the processing of such data must be met in order to justify an exception on the general prohibition on the processing of sensitive data. It is questionable if in practice these conditions are met in all cases where data on trafficked persons and/or sex workers are collected, retained and exchanged. A similar argument can be build for data on trafficked persons’ health status or ethnic origin.