

Safety in Journalism & the Role of the Internet

Initial statement



Gabriel Lansky

I.

Whenever we have mentioned “freedom of the Internet” during the past ten years, we have had to keep the effects of 9/11 in our minds - not only in a moral way but also in a juristic way.

If we focus on the legal situation in Austria and the European Union, we must take into account the point of view of human rights Art 10 ECHR (European Convention on Human Rights) as the main law statute for freedom of expression, as well as the right to respect for private life according to Art 8 ECHR, established in most of our legal systems and reflected in many national laws.

But we must also realize that as an effect of 9/11 as well as of the terrorist attacks on Madrid and London in 2004 and 2005, the EU and national legal framework in this regard has changed, as EU and Member States took action to improve and strengthen their methods and instruments in combating terrorism and organized crime. In many cases the fundamental rights of expression and privacy were restricted during the last ten years in a very serious and often disproportionate manner, not only in Europe but particularly strongly in the US – this all based on the argument of combating terrorism threats.

II. The Influence of 9/11 with regard to the Internet – a US perspective

In my view there are two main reasons indicating why the USA is most affected by cyber-terrorism attacks. On the one hand, the 9/11 attacks occurred on United States soil. On the other hand, the USA (e.g. Silicon Valley) is the country where the Internet originated, further symbolizing the computer era.

It is undisputed that nowadays the Internet is the most significant and fastest-growing communication network in the world. It gives individuals, either alone or in connection with others worldwide, the opportunity to share their own right to freedom of expression with the world. However for many governments, politicians and even the general public, the Internet can be used to feed and support terrorism by making anonymous communication easier and provides a “mass megaphone” for radical messages.

For this reason, the September 11th terrorist attacks prompted US Congressional action on many fronts, and ultimately led to the ratification of the USA PATRIOT ACT on October 26, 2001, which was further prolonged in 2005.

The Act is broadly scoped and vaguely worded, and some of its provisions may be implemented to affect Internet usage, computer security, and critical infrastructure protection, as well as the monitoring of financial transactions.

In the field of computer security, the Act creates a definition for “computer trespasser”, which can be used to describe activities such as a terrorist act in certain circumstances. The Act enables law enforcement officials to intercept the communications of computer trespassers and improves their ability to track computer trespasser activities.

Although the Act does not explicitly address electronic commerce (e-commerce), many of the its provisions have the power to impact online trade. It therefore is said that more can be done to prevent, detect, and prosecute international money laundering and the financing of terrorism. Over time, these provisions may affect e-commerce on a broad scale, and specifically electronic fund transfers.

The Act provides law enforcement officials with greater authority to monitor Internet activity such as electronic mail (e-mail) and Web site visits. While law enforcement officials praise their new authorities for enabling them to better track terrorist and other criminal activity, privacy rights advocates fear that in an attempt to track down and punish terrorists who threaten American democracy, one of the fundamental tenets of that democracy— privacy— may itself be threatened.

Because of the controversial aspects of some provisions found in the Act, particularly regarding privacy, many American organizations are expected to closely monitor how the Act is implemented in daily life. To this regard, we must face the self-evident fact that also journalists are concerned by this Act.

In my view, the following provisions of the USA PATRIOT Act particularly affect Internet privacy and freedom of expression:

- Records of electronic communications were enabled to include records commonly associated with Internet usage, such as session times and duration.
- Cable companies had sought, in particular, to clarify their obligations with regard to release of personally identifiable information about subscribers and whether they were required to notify the subscriber that such information had been requested by a governmental entity.
- It is also allowed and stipulated for Internet providers to divulge records or other information (excluding the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and requires them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions.

- Also routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture, as authorized by a court order, using pen registers and trap and trace devices were allowed.
- It is now also allowed for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances.
- Another clause of the Act allows for nationwide search warrants of e-mail instead of requiring separate search warrants for each jurisdiction in which the e-mail may be located, such as at the Internet service provider location rather than where a crime was committed.

➤ Conclusion:

As noted, the challenge for policymakers was, and still remains, balancing the needs of law enforcement with the desire of the public to maintain its privacy and freedom of expression. In the wake of the terrorist attacks, the public appears more willing to make sacrifices with regard to privacy in order to protect the country against further attacks and bring the perpetrators of the September 11th attacks to justice. Criticism of the USA PATRIOT Act has been relatively muted from a privacy and freedom of speech standpoint, possibly because of the perception that the public is willing to accept such measures at this time.

Other experts and lawyers justly worry that the Act does not include sufficient provisions to deal with potential abuses by law enforcement of the new authorities.

III. The Influence of 9/11 regarding the Austrian legal system

I would now like to provide you with some brief examples concerning the Austrian legal system which demonstrate these – in a way alarming – developments:

> Keyword "data retention"

In spring 2011 the much-debated EU Directive on data retention established in 2006 – as the EU's hasty and rash reaction to the terrorist attacks on Madrid and London – was implemented in the Austrian legal system. In this course of the "Strafprozessordnung StPO" (criminal procedure code), the "Sicherheitspolizeigesetz SPG" (security police act) and the "Telekommunikationsgesetz TKG" (telecommunication law) were adapted.

As of April 2012, all telecommunications and Internet-related data, E-mail connections and mobile phone location data are required to be stored by the provider for at least 6 months, and must be accessible to prosecutors (STA) and the police in order to strengthen their ability to identify and prosecute serious crimes.

That also means that all these communication data – not the content – of every one of us (also including journalists and lawyers) are stored without any suspicion - which in my view has to be seen as an infringement of the right to data protection as evident in Art 8 ECHR and Article 8 EU Fundamental Rights Charter. This is in my view a clear breach of a European law principle and standard, namely that investigations against a person are only allowed in the event of concrete suspicion. Meanwhile, three constitutional courts of EU Member States, namely of Romania, Bulgaria and the Czech Republic, have abolished the respective laws implementing the EU Directive because of a violation of the aforementioned fundamental rights of individuals. It is unfathomable that the 'litmus test', namely with regard to whether the Directive itself conforms to the rights to data protection and privacy guaranteed in the ECHR and the Charter, has not yet been brought before the Luxembourg Court, although all three courts have had the opportunity to do so. However, we expect that the Irish Supreme Court– based on an application of the NGO Digital Rights – will soon initiate a preliminary ruling by the ECJ to this regard.

In this context we must also to be aware that in Austria, based on the current SPG, the police already have permission to monitor personal connecting data (phone, mobile, mail, standpoint) which are stored by the providers for charging reasons for a period of 3 up to 6 months without an order by the court on the basis of exigent circumstances. Although the storage of IP addresses is not covered by the law, in practice, police also gain access to those data from several providers, which is a clear breach of the right to data protection and the right to efficient remedies in this regard because no subsequent information of the individuals concerned takes place.

According to the new § 90 TKG of the court, with the ratification of the aforementioned StPO and SPG amendment in spring 2012, with the approval of prosecutors, the police will further be allowed to request retained data (which are the same as the data stored, but no longer needed for charging reasons, but including IP addresses which are then covered by the law) from the providers. According to the new § 102a TKG, they may use this information for investigation, finding and prosecution of offences, if the crime causes imprisonment of more than one year.

Another problem in this context is the fact that also the data of persons whose profession swears them to confidentiality such as lawyers, journalists or doctors must to be stored by the providers.

The new § 93 (5) TKG stipulates that only editorial secrets and other professional secrets must be noted, which is a not very powerful statute.

We must further criticize that the Directive regulates which kind of data must be preserved, but does not regulate who is allowed, and in which way they may use the data.

While all these capacities exist only for criminal law issues and not for civil law cases, in our opinion we must discuss how far this can be seen as an infringement of civil rights, especially of Art 8 ECHR, the right to privacy.

The international community also aims to prevent the abuse of the banking and finance sector.

Therefore not only data retention laws were adopted, also national laws, such as laws concerning money laundering (BWG – Bankwesengesetz) in Austria, and clauses against terrorist financing in 2007 and 2010 were strengthened. Therefore in some cases it is now permitted to break banking secrecy to prevent terrorist financing. ("Know your customer"-Prinzip).

For this reason, § 165 StGB in Austria considers money laundering and includes the storing, investing, maintaining, changing and realizing of assets which result in crimes as criminal offences.

After 9/11 the community also tightened the fight against financing terrorism with the result that § 278d StGB prohibits the providing of assets for terror reasons, regardless of whether these assets are legally or illegally purchased.

As an additional step, the Austrian Ministry of Justice argues that even a public request of a terrorist offence, or to favor such a crime, is prohibited by law. That means that even stating such views on Internet-websites are criminal offences.

At the moment and in conjunction with the terrorist attacks in Norway, the Austrian Ministry of the Interior wants to automatically connect the information of national and foreign security authorities with Internet-data (Anti-Terror-Paket / Daten-Verküpfung).

More often than not, you will also encounter the wrong assumption of, "*nothing to hide, nothing to fear*", which means that the described observation measures seemingly concern only people who have something to hide. However, this is an entirely incorrect conclusion because of the facts – as previously stated – that data abuse and fraudulent use can never be completely precluded.

And further, if we take a look at our neighbor country **Germany**, we see that the German government changed their criminal law concerning the Internet in 2009. To fight terrorism it is meanwhile, for example, illegal to download bomb-building-instructions as well as to publish such manuals, regardless of violent or criminal intent.

As long ago as 1983, the German Federal Constitutional Court ('Bundesverfassungsgericht') confirmed in one of its judgments that the danger of an overpowering governmental observation is the effect that the citizens - because of these measures – are restrained from using their fundamental rights as the freedom of expression.

IV.

Even if Austrian laws have changed, the European Court of Human Rights (ECHR) confirms in its judgments the will to guarantee and strengthen the right to freedom of expression. For the ECtHR, the right of data protection is an integral part of the right to respect private life. In this context it must be remembered that the ECHR continuously states in its case-law that the Convention is a living instrument which must always be interpreted in the light of present-day conditions.

This can be seen, for example, in the following judgments:

Although Article 8 ECHR only refers to 'correspondence' ('Briefverkehr'), in its case-law the Court stated – taking into account the development of technical means of communication – that also communication via e-mail or pagers, as well as phone calls using the Internet (see ECtHR judgments *Taylor- Sabori v. UK* and *Copland v. UK*), are protected by Article 8 ECHR. The dynamic approach of the ECtHR towards the ECHR can already be shown by the assumption that Article 8 ECHR includes also the right to data protection. This was made clear by the Court already in 1987 in the judgment, *Leander v. Sweden*, picking up the threats for privacy by processing personal data.

At this point I would also like to note the ECHR judgment "*Klass gegen Deutschland*" from 1978, which cautioned governments and countries to not create a system of observation and policing for security protection of the citizens which subverts democracy because we should never forget that in many cases the fact of having freedom (of expression) also implies security.

V.

The demand for safety in journalism means, *inter alia*, that the Internet has to remain a free and unobserved space which must not be used – or better: misused – by police authorities and intelligence services to purchase information sent to or by journalists in the frame of their professional tasks. We know of numerous cases in totalitarian States in which the arbitrary detentions or the murdering of journalists were ordered as a consequence of illegal secret surveillances of the correspondence of media enterprises on the Internet – in particular by reading messages and information sent to journalists which might build a threat for political interests and politicians due to explosive confidences.

When we talk about safety in Journalism and the role of the Internet as lawyers, we must also balance the rights of journalists and victims on one hand, and the perpetrator of a crime on the other. The right to freedom of speech (freedom of press) and the rights of victims according to media and criminal law produce a particular gap between the situation in theory and in reality. Nowadays not only journalists claim their rights to freedom of press. More and more victims, witnesses and even perpetrators of crimes make use of their right to freedom of speech over the Internet.

As a law firm in which we represent the biggest media houses in Austria, we of course usually have to take care of the legal interests of journalists.

In general, data retention and the observation of the Internet concern journalists in various ways. Not only the Austrian editorial secret ('Redaktionsgeheimnis') regulated in § 31 MedienG as an impact of freedom of press and the compliance of the journalistic duty of care are in danger, there are – as already said – risks regarding personal and data privacy rights.

VI.

In some cases, however, it is also our responsibility to fight against criminal webmasters and illegal websites as we successfully did against the NAZI-website, alpen-donau.info, and alpen-donau.net.

In the case against "alpen-donau", (Austria's most famous and notorious neo-Nazi website), we gave legal advice to the Jewish community of Vienna (IKG) as well as to other clients.

Especially individual journalists were threatened by the neo-Nazis on a regular basis in Austria and it was therefore, aside from the legal efforts to achieve a shutting down of the website, furthermore of utmost importance for us to capture the state attorneys' as well as the police's attention, and maintain their awareness concerning those individuals and their families who are threatened by neo-Nazis.

As for the website's infringements of Austrian law, both the Austrian Criminal Code (StGB) and the Austrian Law on Prohibition of Revival of Nazi Activities (Verbotsgesetz) were broken by the authors of alpen-donau.net on a regular basis.

We could achieve the shutting down of these websites as the result of our criminal complaint and procedures based on different laws because on the one hand, the authors were committing a provable copyright infringement under Austrian law (photos were illegally used). On the other hand, such hate speech is illegal even under the restrictions of US free speech rules.

Although there is no enforcement agreement between Austria and the US, we could achieve an arrangement between the government of Austria and the webhost in the US which warrants the shutting down of these illegal NAZI websites.

VII.

The past and the example above show that not only social media platforms and anonymous blog sites, but also "professional" websites, can be used as dangerous platforms for radical and illegal ideas. That's why we need a broad understanding of how the Internet works in order to set legal measures in the correct way for the benefit of the clients.

We therefore need strong bi- and multilateral agreements on behalf of law enforcement, which still are missing, in particular between the EU and its Member States and the US (where of course the most social media companies and blog sites are hosted and located). We, as lawyers, can save our clients using the local and trans-European legal framework

only if legislative power sets the right long-ranging measures in bi- and multilateral enforcement treaties,

Legal wishlist – de lege ferenda:

- Prohibition of acting anonymously over the Internet (Recent initiatives of Facebook)
- Bi- and multilateral agreements for enforcement of court decisions especially, with states such as the US and other countries frequently-used by perpetrators

Measures to be taken by governments and politicians

- Raising awareness of the fact that you still commit a crime when you commit it in the World Wide Web
- A strong monitoring also of providers, police and even the prosecution to prevent fraudulent use

Points to be discussed:

- How can we keep the balance between the public interests of a journalist's work, keep journalists safe, and not reduce the right of freedom of speech at the same time? (Anonymität muss fallen).