Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

# Legal Basis for Social Media

## Report of the Federal Council in Fulfilment of the Amherd Postulate 11.3912 of 29 September 2011

## Summary

Social media or networks are more or less open, interactive and participatory platforms that allow users to communicate as well as to establish and maintain relationships. With little expenditure, users can generate content either alone or together with third parties, make it accessible to others and share content from and about third parties. This is blurring the boundaries between author, producer, distributor and user as well as between private and public communication. Social media is financed primarily through revenue generated by selling the data entered by users on to companies for advertising purposes.

This report presents international standards and recommendations in response to National Councillor Amherd's question regarding the current legal status in relation to social media. It goes on to analyse existing Swiss legislation. It comes to the conclusion that there is currently no need to create a separate special law on social media comparable to that for the radio and television sector. The number of opportunities and threats associated with the new communication channels has resulted in a diverse overall picture. Experience to date has shown no major gaps in Swiss law. With careful application, the provisions of existing laws (e.g. the FADP, SCC, CC and UCA), which are often worded generically, allow a reasonable response to most problems that social platforms might create for individuals and the general public.

However, whether the existing provisions will work in practice is uncertain. This applies primarily to the enforcement of existing legal claims in the event of a dispute, which, given the international nature of the platforms, the often anonymous communication and occasional difficulty of allocating the responsibility of the different parties involved (users, platform operators, providers), could be precarious. The transnational background means that Swiss legislation has limited influence in many places. In some areas, however, it is possible that certain legislative amendments could improve the situation. This applies to individual aspects of data protection, protection of young people from the media and allocation of responsibility of service providers that enable access to networks (platform operators and providers).

Several of these areas are currently the subject of in-depth investigations relating to issues including communication on social platforms. As part of the on-going revision of the Data Protection Act, any need for legislative action in relation to social media will also be established. The review of the effectiveness of existing measures to protect young people will take place as part of the national "Jugend und Medien" [Young People and the Media] programme.

An in-depth investigation into the need for specific rules for the legal responsibility of platform operators and providers is also urgently required. If this analysis reveals that it is necessary to amend the law, an appropriate consultation paper will be submitted.

Aspects of social media with significance in terms of telecommunications legislation will then be addressed in the consultation paper on the revision of the Telecommunications Act, which will be commissioned during the current legislative session according to the Federal Council's current plans.

As previously mentioned, the various activities and investigations concern not only social media, but are to be considered in the context of the legal system as a whole. However, the various aspects must be combined to create a coherent overall picture which also takes account of social media. The flow of information between the governmental offices involved must therefore be ensured. Furthermore, a review of the current position concerning the legal basis for social media would seem advisable, as soon as the aforementioned work is complete and the direction it is going in is clearly visible.

# Contents

# 1 Introduction: Amherd postulate 11.3912

In her postulate[1] of 29 September 2011 Viola Amherd, a member of the National Council, pointed out that social media is creating a new dimension in communication and in media use that threatens to undermine the enforcement of national laws and fundamental rights. According to Amherd, this development in particular concerns rules on data protection, racism, or more generally the protection of privacy and may have to be countered with social media regulation.

The member of the National Council therefore instructed the Federal Council by submitting the postulate calling for a report on the legal status in relation to social media to be drafted in order to answer the following questions in particular:

What is the current legal status in Switzerland and internationally in terms of social media?

- Where are there gaps in the law? How they can be closed?
- How does the Federal Council view the creation of a separate Social Media Act that takes into account the specific characteristics of these new forms of communication?

In its Opinion of 23 May 2011, the Federal Council questioned whether existing legislation (in particular in the FADP, CC, SCC and CopA) adequately addresses and sufficiently clarifies the responsibilities of those involved. This applies for example to protecting users struggling to cope with the challenges of social media from the undesired use of their data and the often inadequate options for transferring their data from one social media platform to another. Another central issue is the enforcement of existing laws, as the operators of social media platforms are often international and national legislation is therefore reaching its limits. The Federal Council agreed to accept the postulate.

This report has been prepared under the auspices of the Federal Office of Communications. The work was carried out in coordination with the Federal Office of Justice, the Swiss Coordination Unit for Cybercrime Control (CYCO), the Federal Social Insurance Office and the Federal Office of Public Health, as well the expert group on the revision of the Data Protection Act. Three external expert opinions (on conceptual questions about social media, on enforcing the law in an international context and on private individuals whose rights have been violated) have been incorporated into the content of the report.

[1] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912 (only available in German, French and Italian).

# 2 Social media (social networks)

## 2.1 Definition

Social media or social networks[2] have in recent years spread rapidly all over the world due to broadband internet. Social networks are also used extensively in Switzerland. 47% of Swiss citizens log on to online communities or private online social networks; 22% use online networks professionally and 11% use the micro blogging service Twitter[3]. Two thirds of Swiss companies, authorities and organisations maintain an active social media presence and only 34% have no presence on the social web[4]. Social media and social networks are more or less open, interactive and participatory platforms that allow users to communicate as well as to build and maintain relationships. Moreover, social networks users can share information and content from and about third parties as well as generate content themselves or in association with others and make it accessible to other users with little expenditure. In Switzerland, more than a million people produce and share their own content on the internet; uploading photos and videos enjoys great popularity in particular[5].

The different forms of social media are constantly expanding, which – depending on the respective platform architecture created by the operators and the networking opportunities with other platforms – can open up different possibilities of use, interaction and co-creation of the platform itself.

Social media often allows unplanned collaborations whereby users recognise other users' content as relevant to them and then act on it, enhance, process and place it in new contexts. This can result in large collaborative works without any preliminary planning[6].

However, most social network users focus on sharing private information with a small circle of people, most of whom they know. At the same time, however, the same social networks are often used for professional or journalistic communication with the aim of influencing the purchasing behaviour of consumers or public opinion.

The opportunities social networks provide for shifting boundaries are increasingly regarded as their most salient feature; compared to traditional communication channels and media, this applies to three areas in particular:

### 2.1.1 Blurring of the boundary between author, producer, distributor and user

While in traditional media a clear separation between service providers (e.g. professional editors, film directors, media companies) and users (the public) tends to prevail, social network users can easily switch between producer and consumer roles. Amateurs can individually or jointly create content or modify the existing content of third parties and decide on distribution to other users.

### 2.1.2 Blurring of the boundary between private and public communication

Traditionally there are separate channels for private and public communication: In private communication the sender usually knows the receiver(s) (e.g. in person, by letter or in telephone conversations). In public communication the sender does not usually have precise knowledge of the receivers.

---

[2] The two terms are used interchangeably for the purposes of this report.

[3] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. University of Zurich, Zurich, p. 16, 19.

[4] Bernet ZHAW Studie Social Media Schweiz 2012, p. 3ff.; available at: http://www.bernet.ch/socialmediastudie (only available in German).

[5] Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. University of Zurich, Zurich, p. 17f.

[6] Aguiton C./Cardon D., p. 52.

Many social media sites allow users to easily switch between private and public communication on the same platform. This is reinforced by the fact that traditional mass media is also present on social networks and can help users achieve a mass media effect when they act on and share these.

### 2.1.3 Blurring of the boundary between local and remote data processing

Social media relieves users of the need to store their data and content in a particular physical location. Data and content that is uploaded onto social networks is available to users wherever they have access to the relevant network. The storage of content on third-party servers leads to greater flexibility and efficiency of use, but often goes hand in hand with a certain loss of control of (personal) data and content.

## 2.2 Categorising social networks

Due to the variety of platforms, their different features and complexity, and their continuous development and change, a clear division into categories is almost impossible. In addition, social networks escape simple classification because they are neither a pure development of traditional mass media, nor are they a means of communication exclusively for individual communication[7]. In research, social media is often categorised according to the following criteria:

### 2.2.1 Functions of social media

Social networks are often categorised according to their functions, although they frequently have multiple functions. In research there are various categorisations, which as a minimum distinguish between content- and relationship-oriented features.

2.2.1.1 Content-oriented functions

- Information and knowledge management:
  creating, detecting, receiving, managing and exchanging opinions, knowledge and information, e.g. wikis, social bookmarking, tagging, RSS, blogospheres or special interest sites[8].

- Entertainment or experiencing virtual worlds:
  exchanging content with the purpose of entertainment or of experiencing virtual (game) worlds, such as YouTube, certain interactive online games, etc.

2.2.1.2 Relationship-oriented functions:

- Relationship management: maintaining existing and establishing new relationships (e.g. on contact platforms), linking of people with similar interests and exchanging information , e.g. special-interest sites such as Myspace for musicians.

- Identity and reputation management: (selectively) presenting aspects of one's own person, e.g. on personal blogs, podcasts, etc.

### 2.2.2 Opportunities for participation in social media

Another method to categorise social media is based on the technical options available to users to participate on social networks. Two aspects are considered as criteria: Firstly, the degree of co-creation of the exchanged content, which can range from the mere possibility of rating or commenting up to the creation or modification of content. Secondly, the degree to which communication is public, which can range from purely individual to publicly networked mass communication.

---

[7] Neuberger, Christoph, "Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick". in: Neuberger, Christoph; Gehrau, Volker (eds.): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, p. 34.

[8] Schmidt, Jan, "Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen", in: Zerfass and others (eds.): Kommunikation, Partizipation und Wirkungen im Social Web, Bd. 1, Cologne 2008, p. 71.

### 2.2.3 Social network revenue models

Social networks are not subject to the law of scarcity, but work exactly in reverse: the value of a product or service increases with the number of users. This is known as the network effect[9]. Network effects can be observed for different players in the offerings of social networks. With an increasing number of members the opportunity to meet like-minded people increases for all users, as does the appeal for developers to provide applications for the platform; for advertisers the likelihood of being able to address narrowly defined target groups increases. For these reasons social networks often first rely on a strategy that can quickly gain them a large number of users without generating significant revenue. They attempt to bind these users to prevent them migrating, or make it more difficult for them to migrate, to other networks.

Due to the economies of scale of these networks and forums, there are major incentives to acquire and amalgamate with other media in order to operate as profitably as possible. This can – at least for a limited time – lead to market dominant positions for a few individual platforms.

Social media revenue models can be divided into commercial and non-commercial forms. There is a tradition of free use of content that dates back to the early days of the internet. There are still many social media that do not operate commercially; instead they primarily feel committed to the community concept. As users often understand these networks as a community work to which they owe a certain loyalty, they are often willing to fund the upkeep of the respective platform via donations. Another form of non-commercial funding of social media is via the public sector, as it may be in the public interest to establish special services on social networks for specific target groups such as children and young people.

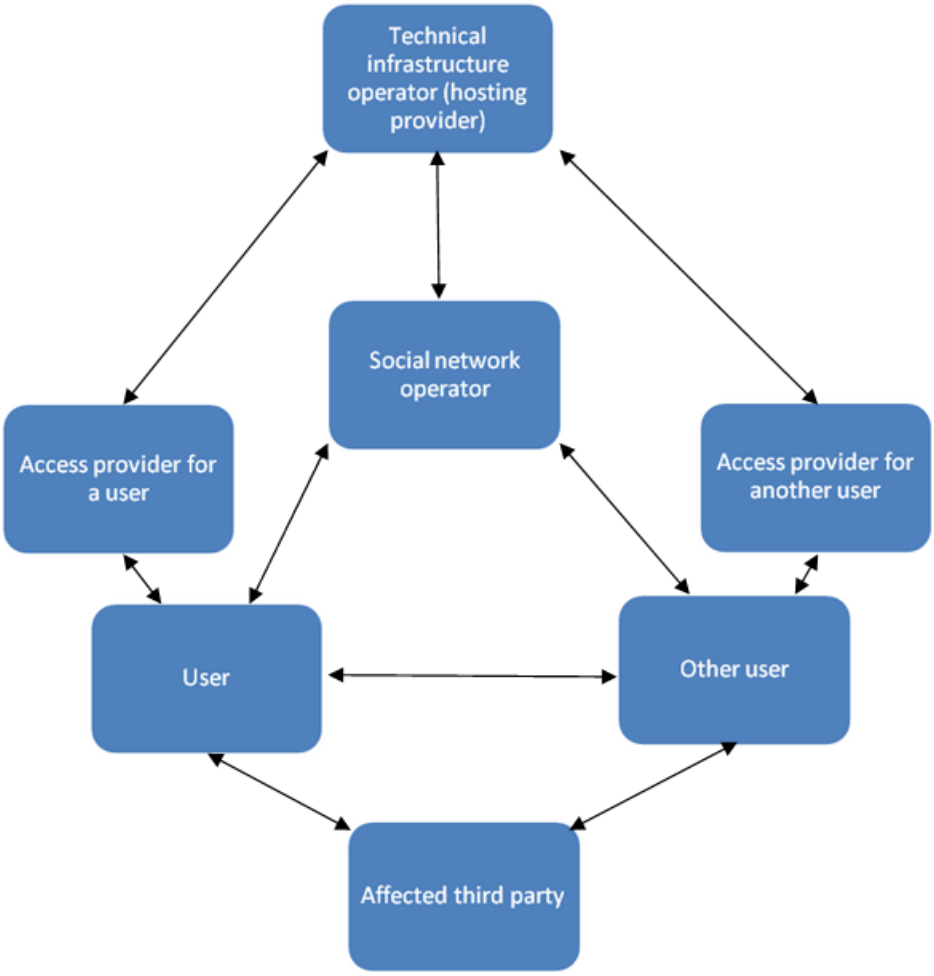
Commercial social media revenue models include, in particular, funding through user fees and advertising. Funding through advertising predominantly involves advertisements that are dynamically adapted to the respective content on the screen to attract users' attention. Static advertising is used to a considerably lesser extent. As social network users create a profile with information about themselves, a relatively large amount of data about them is available. The details entered are sold to companies for advertising purposes. Precise targeting is possible through the creation of profiles. Advertising is charged either per 1000 views or in accordance with the cost-per-click method, where the advertiser pays only when those targeted click on the advertisement. The target groups of specialised platforms[10] have a higher financial value. Users therefore "pay" with their personal data for free use of the services that social media provide.

[9] Rimscha M. Björn, "Geschäftsmodelle für Social Media" in: Grimm, Petra; Zöllner, Oliver (eds.): Schöne neue Kommunikationswelt oder Ende der Privatheit? Stuttgart 2012, p. 303 f.

[10] For example, platforms directed at the professional world, such as Xing and LinkedIn.

## 2.3 Roles in relation to the use of social networks

There are many different parties involved in social networks, each with different roles. It should be noted that in practice the different roles are not always clearly defined. The transitions between these functions are often fluid,[11] which means that platform operators can also act as hosting providers. However, the following, simplified classification serves as a basic initial overview :




### 2.3.1 Operators of social media network platforms (platform operators)

Operators of social networks (platform providers) provide users with a framework to share content they have created themselves or have acted upon. Many of the platforms that are most heavily used in Switzerland have their headquarters abroad. Among the best known *foreign* platform operators are Facebook, YouTube and Twitter. However, there are also *Swiss* platform operators. These include providers of blogs, which are sometimes prosecuted before Swiss courts for problematic posts (e.g. the SRG[12] or certain newspaper publishers[13]).

Operators determine the options for interaction and dissemination of content via the architecture and design of the platform. They also determine the extent to which users can create private, semi-public and public spaces for communication and exchange they exchange content between these spaces.

---

[11] cf. the comments on the various parties involved in internet communication in the report by a commission of experts on "Netzwerkkriminalität" [Network Crime], FDJP 2003, p. 27ff.

[12] cf. the dispute over a defamatory comment on the blog of the television show Alpenfestung (Decision of the Swiss Federal Supreme Court 136 IV 145).

[13] cf. the dispute over a politician's post that violated personal rights on a blog platform operated by the Tribune de Genève (FSC 5A_792/2011 of 14/01/2013).

Operators can focus on directing users' attention to specific content via "content rankings" and links to third party content. In addition, operators determine what data they collect from users, which rights to the exchanged data and content they acquire and how they use these economically.

Most platform providers set user rules for dealing with other users or unaffiliated third parties as well as the creation, use and sharing of content. Operators can specify what content or forms of behaviour are undesirable or prohibited via the terms of use. However, in practice they usually exercise less editorial control than traditional media. While traditional media content is usually selected by an editorial board in advance (*ex-ante*), control on social networks is usually *ex-post*, whereby content that contradicts the conditions of use or is subject to the criticism of other users can be retrospectively removed ("notice-and-take-down"). Citing their users' personal responsibility and organisational skills, certain platforms leave it to users to define these rules themselves.

### 2.3.2 Technical service providers (e.g. hosting and access providers)

Communication via social networks relies on a technical infrastructure. Some platform operators store the resulting data on their own servers. However, many platform providers employ the services of a third party, which provides them with the technical infrastructure (storage space, computer capacity, transmission capacity) for the automated linking of data (often a **hosting provider**). Like most of the platform operators with a strong presence in the Swiss market, the majority of hosting providers are also based abroad. They usually have no editorial responsibility of their own, but (depending on their configuration[14]) are technically capable of *deleting* content that is stored on their computers and recognised as undesirable.

The connection between the computers of social media users and the servers with the platform data is established by **access providers**. They have a contract with the users. Swiss users usually use the services of a Swiss-based access provider. One of the best-known access providers is Swisscom. Access providers are not usually able to delete unwanted content (since they are not stored on their servers). However, it is conceivable, that they could specifically block access to certain content.

### 2.3.3 Users and sharers

It is essentially users who create content ("user-generated content") or link to content created by others. To do this they require the technical support provided by the access provider and access to the relevant social media platform. They can usually decide to whom they direct their communication, i.e., whether they wish to share their content with the general public or only with a select group of people. They are operating within the technical possibilities and content specifications provided by the platform operators.

From the operators' perspective, users have a (joint) responsibility for the way they treat each other and for the content that they make available to a wider audience on social networks. User liability for activities that violate legal principles or the rights of third parties is often not clearly defined or not known to the users. This may lead to risks for those involved and the affected users.

### 2.3.4 Affected third parties

Third parties that are themselves not active on the respective networks may be affected by social media activities. This is the case when content affecting third parties is transferred from social media to the mass media or when network members use data on social networks via a third party without obtaining permission.

[14] Sometimes the hosting provider cannot delete individual content on a server they have rented out; they can only turn off the power or physically remove the hard disks, which is often likely to be disproportionate action.

### 2.3.5 Traditional (mass) media and other media services

The traditional media often help social media attract attention, recruit new members and increase advertising revenue. In return, social media increasingly serves the traditional media as a supplier of content and news.

These relationships make it even more difficult for social network users to recognise the boundaries between private and public communication. Many conventional media maintain their own social media presence or are associated with or linked to major social networks, e.g. Facebook.

Search engines, which refer users to content both in the traditional media and social networks, also function as "linkers". Economic cooperation also takes place, particularly in relation to exchanging and analysing user data for advertising purposes, etc.

## 2.4 Preliminary notes on the legal integration of parties involved in social media

### 2.4.1 Constitutional rights and obligations

No specific legal regulations regarding communication via social networks have been adopted to date in Switzerland (or in other countries as far as can be seen). Nevertheless, the use of social media does not take place in a legal vacuum.

The legal system guarantees the parties involved in communication (users, but also platform operators and providers) the highest level of protection from government interference. The Swiss Constitution and the European Convention for the Protection of Human Rights and Fundamental Freedoms guarantee unhindered communication (Art. 16, 17, 21, 22, 23, 34 of the Federal Constitution and Articles 10 and 11 ECHR) and economic freedom (Art. 27 of the Federal Constitution). The freedoms guaranteed by these fundamental rights are not absolute; they may be restricted by the government. Strict conditions should therefore be observed by the authorities. According to Art. 36 of the Federal Constitution, restrictions on the right to freedom must have a legal basis and must be in the public interest or serve effectively to protect the fundamental rights of third parties in a proportionate manner. Interfering in the core content of fundamental rights, such as the systematic censorship of communication content by the government is absolutely prohibited (Art. 17 para. 2 of the Federal Constitution).

In regard to communication via social media by private individuals, the government is bound by two commitments: first, it must not violate the fundamental rights itself; second, it must protect the rights of private individuals from undue restrictions by other private individuals.

The use of social networks provides opportunities and also threats in relation to the various rights of individuals as well as for the common good. In order to protect the fundamental rights of third parties and the public interest (e.g. security and public health[15]), the government must meet certain legal requirements. It must, for example, provide tools to protect against violations of the private and family life (Art. 13 of the Federal Constitution and Art. 8 ECHR) of individuals. Possible examples include the enactment of legal provisions to protect against defamatory or revealing publications.

Children and young people deserve special protection. The UN Convention on the Rights of the Child therefore requires the protection of children against all forms of exploitation that affect their well-being (Art. 36) and guaranties them protection against unlawful attacks on their honour and reputation (Art. 16)[16]. The European Court of Human Rights (ECtHR) requires the government to take effective steps

[15] Possible examples includes measures against alcohol and tobacco advertising and drug abuse.

[16] Convention on the Rights of the Child, adopted in New York on 20 November 1989, entered into force in Switzerland on 26 March 1997 (UNO Kinderrechtskonvention - UN Convention on the Rights of the Child), CC 0.107.

if the private lives of young people are affected by immoral publications on the internet (publication of an objectionable personal advertisement)[17].

Freedom of the press also results in obligations for the government. It must therefore take appropriate action against the abuse of opinion-making power by (economically) powerful private operators.

### 2.4.2 Rights and obligations under existing statutory law

#### 2.4.2.1 Compliance with the general legal requirements

The constitutional requirements are specified at the legislative level. Swiss statutory law contains various provisions that define or limit the rights of the concerned parties in more detail. These rules apply not only to communication on social networks, but also to statements via traditional channels such as newspapers, radio, letters or telephone conversations. Possible examples include criminal, civil (protection of personality) and data protection law. A detailed explanation of the relevant regulations and their implications for social media can be found in Chapter 4 of this report.

#### 2.4.2.2 Specific regulation of platform operators under telecommunications law?

Swiss law has special regulations for certain providers and disseminators of information. This applies to providers of conventional radio and television programme services, which are subject to the provisions of the Radio and Television Act (RTVA).

Specific requirements for the provision of telecommunication services, i.e. the transmission of information by telecommunications techniques for third parties (including radio and television programme services) can be found in the Telecommunications Act (TCA). Anyone providing a telecommunications service must, for example, register with the Federal Office of Communications (Art. 4 TCA), fulfil organisational requirements (Art. 6 TCA), maintain telecommunications confidentiality (Art. 43 TCA), participate in dispute resolution procedures (Art. 12c TCA), use transparent pricing (Art. 12a TCA), combat spam (Art. 45a TCA) and comply with numerous other obligations. The TCA dates from a time when the provision of telecommunications services was dependent on the possession or at least authorised access to a specific network serving this purpose. The evolution of technology means that this close relationship between network and services is now lifted. Today there are completely different technical conditions (e.g. internet, smartphones). Services may be provided in various ways and without the active intervention of network operators; this has opened up the possibility of entirely new business models (e.g. funding through advertising).

Under current law, anyone who transmits information between at least two other parties is a telecommunications service provider (Art. 3 lit. b TCA). Operators of social media platforms usually do not do this; instead they are one of the parties between which information is transported. However, there are exceptions where platform operators are at least partly responsible for the transmission of information between third parties; in this case a telecommunications service is indicated according to the definition valid today. An example of this is messages sent from one Facebook member to another using e.g. Facebook Messenger. Apart from the difficulty of enforcing national telecommunications law on international platform operators based outside Switzerland with current legal instruments, many of the existing legal regulations for telecommunications are not tailored to their activities.

[17] ECtHR Judgement "K.U. vs Finland" (Case no. 2872/02) of 02.12.2008: Unjustified refusal of the Finnish judicial system to commit the provider to return the data in question.

# 3 Potential and risks of social networks

## 3.1 General

The increasing presence of social networks in the everyday lives of many people means that they are the subject of discussion and observation by private individuals, states and multilateral organisations. In recent years, bodies such as the Council of Europe and the European Union have become increasingly concerned with their potential and risks.

## 3.2 Potential of social networks

Social networks allow private individuals to produce and disseminate content easily, quickly and cheaply themselves. They offer opportunities for entertainment, cultural and political exchange and to generate income. Moreover, they can contribute to the political activation and mobilisation of the population. Increasing numbers of individuals are given the opportunity to participate in public discourse[18].

The *European Court of Human Rights* has emphasised that the internet is now one of the most important means of expression and information creation, particularly in relation to political and other issues of general interest.[19]

The *Council of Europe* has drawn up a number of recommendations for its 47 member states to help individuals use the internet and new communication services (including social networks) to improve the protection of their fundamental rights[20]. To achieve this, they are to encourage media literacy[21] amongst the population. In order to raise the awareness of all stakeholders in terms of their responsibility to citizens and to encourage improved cooperation, the Council of Europe increasingly works together with the private sector and civil society in relation to the internet and the new media sector[22].

In its Recommendation on the protection of human rights with regard to social networking services[23], the Council of Europe emphasises promoting freedom of information, expression and assembly through social networks and the various possibilities for improving the participation of the individual in political, social and cultural life. In a recommendation on media pluralism, the Council of Europe also expressly indicated that member states should support the development of social networks to promote media pluralism and spaces for dialogue[24].

In order to ensure the functioning of an independent and pluralistic media system in the information society, the Council of Europe has developed a concept for a new comprehensive notion of media that should allow the basic principles that support traditional media regulation to be applied in a modified and scaled-down form to new media such as social networks[25].

---

[18] Quantitative information can be found in Hilty/Oertel/Wolk/Pärli, Lokalisiert und identifiziert, Zurich, 2012, pp. 130f.

[19] ECtHR Judgement "Ahmet Yildirim vs Turkey" (No. 3111/2010) of 18.12.2012 on the blocking of the platform Google Sites in violation of the ECHR.

[20] http://www.coe.int/t/dghl/standardsetting/media/doc/cm_EN.asp.

[21] "Media literacy" means the ability to select and use media to understand and critically evaluate media content, to understand the media industry, to recognise the influence of media and to be able to communicate and make transactions in a variety of contexts.

[22] cf. the human rights guidelines developed in cooperation with internet service providers and online game manufacturers: http://hub.coe.int/de/human-rights-guidelines-for-internet-service-providers-and-online-games-providers/.

[23] Recommendation CM/Rec(2012)4 of the Committee of Ministers of the Council of Europe of 04.04.2012 on the protection of human rights with regard to social networking services (Council of Europe Recommendation on social networking services).

[24] Recommendation CM/Rec(2007)2 on media pluralism and diversity of media content. The European Court of Human Rights led to this suggestion in its Judgement "Centro Europa 7 S.R.L. & Di Stefano vs. Italy" (No. 38433/09) of 07.06.2012 (Clauses 72, 134), for example, the subject of which was insufficient media pluralism in Italy.

[25] Recommendation CM/Rec(2011)7 on a new notion of media.

*EU institutions also* deal with the diverse potential of social networks, highlighting, for example, the huge benefit of social platforms for realising human rights, for political participation[26] and for independent media coverage[27]. Similarly, they also emphasise the innovative and creative content of social networks and their importance for the economy[28] and call for the creative use of this media to be fostered[29].

## 3.3 Risks posed by social networks

However, due to the dominant position of a few global platforms, risks may also arise, e.g. the diversity of information and opinion may be reduced and market dominance of a social network may be abused for political or economic purposes. Moreover, the content shared via social networks harbours various risks for individual and general interests (for details see Chapter 4 of this report).

The *Council of Europe Recommendation* on social networking services sees the risks of social networks primarily in areas such as possible discriminatory administration of social platforms, risks to children and young people, the lack of protection of privacy and insufficient data protection.

The *European Economic and Social Committee (EESC)* also identifies the lack of protection of privacy and of children and young people as a key problem posed by social networks[30]. It recommends the introduction of self- or co-regulatory provisions by EU institutions, which are to be converted into binding regulations in the event of insufficient implementation. Due to the dynamic development of social networks, the EESC is calling for the formulation of general, technologically neutral rules for the regulation of platforms and supports the comprehensive promotion of digital literacy for the population and the expansion of internet hotlines to monitor improper activities on social networks.

---

[26] Gemeinsame Mitteilung Menschenrechte und Demokratie im Mittelpunkt auswärtigen Handelns, KOM(2011) 886 endgültig, p. 14, 20f. [Joint Communication "Human rights and democracy at the heart of the EU external action, COM(2011) 886 final], Stellungnahme des Ausschusses der Regionen "Universaldienst im Bereich der elektronischen Kommunikation" and "künftige Netze und das Internet", ABl. C, 28.05.2009, p. 41 [Opinion of the Committee of the Regions on universal service in electronic communications and future networks and the internet, OJEC C, 28.05.2009] and Empfehlung EU-Parlament zur Stärkung Sicherheit und Grundfreiheiten im Internet, (2008/2160(INI)), ABl. C 117 E, 06.05.2010, p. 206 [Opinion of the Committee of the Regions on universal service in electronic communications and future networks and the internet, (2008/2160(INI)), OJEC E, 06.05.2010].

[27] Entschliessung des Europäischen Parlaments vom 07.09.2010 zu Journalismus und neuen Medien – Schaffung eines europäischen öffentlichen Raums, ABl. 308 E, 25.10.2011, p. 55. [European Parliament Resolution of 7 September 2010 on journalism and new media – creating a public sphere in Europe, OJEC 308 E, 25.10.2011].

[28] Opinion on the Internet of Things, OJEC C 77, 31.3.2009 p. 60 or Mitteilung "Bericht über die digitale Wettbewerbsfähigkeit Europas Hauptergebnisse der i2010-Strategie 2005-2009", KOM(2009) 390 endgültig, p. 10 [Communication "Europe's Digital Competitiveness Report: Main achievements of the i2010 strategy 2005-2009", COM(2009) 390 final].

[29] Schlussfolgerung zur Förderung des Kreativitäts- und Innovationspotenzials junger Menschen, 2012/C 169/01, p. 2 [Conclusions on fostering the creative and innovative potential of young people, 2012/C 169/01]. See also Mitteilung "Bericht über die digitale Wettbewerbsfähigkeit Europas Hauptergebnisse der i2010-Strategie 2005-2009", KOM(2009) 390 endgültig, p. 12 [Report on Europe's Digital Competitiveness Report: Main achievements of the i2010 strategy 2005-2009, COM (2009) 390 final, p.12] or Stellungnahme "Eine digitale Agenda für Europa", 2011/C 15/07, p. 38 [Opinion on a Digital Agenda for Europe, 2011/C 15/07].

[30] Stellungnahme "Verantwortlicher Umgang mit sozialen Netzwerken und Verhinderung der durch soziale Netzwerke verursachten Probleme", ABl. C 351, 15.11.2012, p. 31 [Opinion on the Responsible use of social networks and preventing the problems caused by social networks, OJEC C 351, 15.11.2012].

# 4 Current legal status in the social network sector

## 4.1 Preliminary note

As shown above, social networks can be of great benefit in the modern information society. At the same time, however, the use of social networks also harbours risks, including some legal risks. In the following, several specific problems of social networks are discussed in relation to the interests of users, other persons indirectly involved and the general public. Furthermore, selected solutions to these problems are presented for foreign countries or international law, the current legal status in Switzerland is also analysed.

## 4.2 Discriminatory administration of social networks

### 4.2.1 Problematic access conditions and denial of access

#### 4.2.1.1 Background

The use of social networks often requires the disclosure of personal information (e.g. name or e-mail address). The scope and content of the required information may vary depending on the platform. The typical business model (marketing of customer data) and the interest in opportunities for controlling the communication that takes place on the network means that many platform operators are interested in truthful information about the identity of the users. Although interested persons sometimes avoid the rules established by the operators to disclose personal information, the majority of users are likely to give truthful information about their identity on social media platforms. The disclosure of this information can be problematic when there is a lack of transparency regarding the further processing of the data concerned.

Registration data may also contain information about future users that allows conclusions to be drawn regarding aspects of their identity; this might result in the platform operator denying them access. This would be particularly problematic if an exclusion of this kind were to be based on the affiliation of users to a particular group (e.g. defined by characteristics such as race, nationality, political opinion, religion, sexual orientation, gender, etc.).

It is also possible that certain undesirable individuals or companies could be excluded as a result of other, e.g. economic interests. However, as the business models of most social networks benefit from the largest possible membership, the denial of membership tends to be the exception.

#### 4.2.1.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services warns against discriminatory practices on social networks, such as the possible exclusion of users from the platform.

#### 4.2.1.3 Legal status in Switzerland

The principle of freedom of contract means that private individuals are generally free to determine whether, with whom and for what content they wish to enter into a contract[31]. Under Swiss law, platform operators are in principle free to decide which contractual partner they accept. However, freedom of contract has its limits, e.g. a provider may in specific cases be obliged to conclude contracts with interested parties (obligation to contract).

The obligation to contract is expressly regulated in Article 261$^{bis}$ SCC, according to which it is illegal for any person to refuse access to any service they offer that is intended for the general public to any other person or group of persons on the basis of their race, ethnicity or religion (e.g. if a platform operator were to exclude a community of interest because of their ethnic background ). Similarly Art. 6 of the Federal Act on the Elimination of Discrimination against People with Disabilities (DDA, CC 151.3) prohibits public services offered to private individuals from discriminating against disabled persons

[31] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6th ed., Bern 2012, p. 171f.

because of their disability. Those concerned may apply to a court for compensation (Art. 8 para. 3 DDA). The law also allows disabled people's organisations of national importance to take civil action in order to determine discrimination (Art. 9 para 3 lit. a DDA).

The obligation to contract under private law can be derived from the protection of personality under civil law (Art. 28, 28a para. 1 no. 2 CC) and the prohibition of immoral damage (Art. 41 para. 2 of the Code of Obligations)[32]. The prerequisite is that the offering party offers on the open market and to the general public the goods or services that are part of normal requirements[33], the requesting party has no reasonable alternative due to the provider's strong position of power and the provider can specify no objective grounds to refuse the contract[34].

The Cartel Act[35] also restricts freedom of contract, but only for market dominant companies. Increasingly, companies use social media services, particularly for the purposes of advertising and contacting customers. If, for example, a social network were to have a dominant position in the advertising market, preventing access to interested companies could possibly be contrary to the Cartel Act as a denial of a business relationship (Art. 7 para. 2 a CartA).

The analysis indicates that when concluding contracts, private individuals enjoy a wide range of freedoms under Swiss law (with respect to contractors, content, etc.). This freedom is limited by the law, however, when one of the parties achieves a dominant position on the market or if the contract is denied due to certain characteristics on the part of the counterparty. In these cases, the contract can be enforced legally.

### 4.2.2 Censorship of content by social network operators

#### 4.2.2.1 Background

Many operators of social networks provide in their conditions of use rules of conduct for communication on their platform and a list of certain generally prohibited content. Pornographic, racist, discriminatory, insulting and excessively violent content is usually prohibited. Social networks that are available worldwide often design their content controls in such a way that they are in line with the legal systems of most countries in terms of illegal content. This may mean that certain content is deleted even in countries in which it would not have posed a legal issue.

The control methods are different in nature. For example, suspicious content may be reported by users and then examined by the operator and possibly deleted. Operators also often use filtering software, which automatically censors content. It is also possible to permanently delete user accounts as a result of infringements. All these methods can lead to essentially harmless content being deleted (e.g. a photo of a nursing mother). This is particularly problematic in cases where the published and shared content is neither illegal nor socially harmful or is shared in restricted user groups.

#### 4.2.2.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for users to receive transparent information on the editorial criteria for content control of platforms and on the process for dealing with seemingly illegal or undesirable content and forms of behaviour; it also stipulates that the control mechanisms used must not lead to inadmissible restrictions on freedom of expression and information. In its Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers, the

---

[32] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6th ed., Bern 2012, p. 179.

[33] Goods and services that are now available to virtually anyone and used in everyday life. See Decision of the Swiss Federal Supreme Court 129 III 35 E. 6.3.

[34] Decision of the Swiss Federal Supreme Court 129 III 35 E. 6.3.

[35] Federal Act of 6 October 1995 on Cartels and other Restraints of Competition (CartA), CC 251.

Council of Europe also warns against the possible danger of internet service providers restricting the fundamental rights of communication of their customers as a consequence of political pressure and draws the attention of the member states to the gravity of the possible restrictions on fundamental rights. Furthermore, the Council of Europe calls for users to be informed about the use of content filters on the internet as well as to be given clarification and appeal rights with regard to the use of filters and in some cases control over content filtering[36].

#### 4.2.2.3 Legal status in Switzerland

Within certain legal limits, those who transmit third-party content enjoy freedom to decide which content they wish to transfer. The Radio and Television Act and the Telecommunications Act lay down specific limitations that establish certain obligations of transmission. Platform operators, however, are usually not subject to these regulations. Moreover, issues of competition law could be raised: in the case of private companies with a dominant market position, a refusal to transmit certain content may unlawfully hinder third parties in the course of the taking-up and pursuit of the competition if the market dominant company cannot provide any objective reason (e.g. illegality or immorality of content to be transmitted, lack of space, etc.) for rejection (Art. 7 Cartel Act, CartA). If a social network finds itself in a dominant position and for this reason is able to arbitrarily decide on the transmission of content, the question is whether – analogous to the content obligations of radio and television broadcasters or the obligation on telecommunications service providers to transmit specific programme services – obligations regarding the transmission of content can be justified. A legal obligation for platform operators to transmit certain content restricts their fundamental rights (e.g. economic freedom) and requires the usual justification (Art. 36 of the Federal Constitution).

In certain circumstances copyright (i.e. moral rights) or the protection of personality under civil law (Art. 28 CC) may be used to counter the deletion of certain content.

The government can also indirectly restrict the fundamental rights of communication by obstructing private individuals from exercising them. It is therefore conceivable that strict content control by a platform operator could also be indirectly attributable to the government. In particular, an ambiguous legal status in the form of vague legislation could mean that private individuals are not clear about which expressions are permitted by law[37]. Ambiguous regulation of the liability of providers and platform operators regarding their responsibility in relation to illegal content transmitted by third parties could in cases of doubt lead to the deletion of posts that pose no legal issue in order to avoid potential legal problems.

## 4.3 Impairment of other individual interests by platform operators

### 4.3.1 Fundamental problem: Lack of control of users over their data

#### 4.3.1.1 Background

From a data protection point of view, the insufficient control users have over their data is a central problem[38]. The manifestations of this lack of control are manifold:

The scope of users' autonomy in relation to the use of their data depends not only on their decision on whether to join a social network and what information they reveal about themselves there[39], but the

---

[36] Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to Internet filters.

[37] Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4th ed., Bern 2008, p. 376.

[38] cf. the Report concerning the evaluation of the Federal Act on Data Protection of 09.12.2011, (BBl 2012 335, 350). A study conducted by Stiftung Warentest, which investigated ten frequently used social networks in relation to criteria such as "organisation and transparency", "dealing with user data", "data security", "user rights", "protection of young people" and "deficiencies in Terms & Conditions" pointed to various deficiencies in the areas concerned. The US platforms Facebook, LinkedIn and Myspace and German networks such as Xing and StayFriends fared poorly. See Stiftung Warentest "Datenschutz bei Onlinenetzwerken", 2010; available at: http://www.test.de/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-0/ (only available in German).

software offered by the platform operators is more important: it regularly limits users' control over their data by way of poor default privacy settings. Another problem is that it is possible for third parties with access to other user profiles to post photos and text on these profiles without the prior consent of the profile owner or to download content accessible from user profiles without asking.

Users' control over their data is also withdrawn and made difficult by means of extensive consent requirements for data processing. The frequent introduction of new applications and services and regular changes in the conditions of use and privacy statements also lead to the fact that users constantly have to gain new information in order to stay up-to-date with current data processing methods. Information on the use of profile data and transaction data is frequently difficult to find and there is often a lack of transparent explanation for users concerning the purpose of data processing, the possible transmission of data to third parties and simple mechanisms for the enforcement of access and correction rights.

Even the privacy of individuals who do not use social networks is usually only guaranteed to an insufficient degree. Certain network operators (namely Facebook) allow users to upload to their user profile their contacts from phone and e-mail address lists and instant messenger services (friend-finder function). This allows the platform operators to determine which of the uploaded contacts are not yet members of the network. Usually, the platform uses the addresses given with the consent of the member to send referrals and advertising to non-members (these are unsolicited by the recipient).

The granting of extensive powers to the platform operator in the General Terms & Conditions (T&Cs), to which users must usually agree in order to use the service, leads to further restrictions on control. If there is a shortage of social networks or the use of alternative platforms is of limited interest due to their low number of members, restrictive conditions of use dictated by the platform operator are particularly problematic. Many networks grant *far-reaching user rights to user data*. The deletion of content by users, which they can often misinterpret as a permanent deletion of content (including the data on the network operator's server), does not usually make any difference.

An example from the consulting practice of the FDPIC illustrates the disadvantages that insufficient control over data may lead to: the organiser of a major event selected a social network as its primary communication channel, but the platform operator deleted the organiser’s network presence shortly before the event date. As the organiser possessed no contact information about the participants outside the network, it could not provide information on the definitive schedule of this event. Despite the fact it had paid for a network presence, the organiser had not been provided with a direct contact by the platform operator. The organiser was forced to raise its concern via the general contact form and was thus unable to inform the participants in time.

#### 4.3.1.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for platform operators to increase the transparency of data processing, obtain the informed consent of the data subject and inform users about whether their communication is private or public. Moreover, it also recommends the following: Users should be helped to understand social network settings. They should consciously decide the extent to which their data can be accessed by third parties ("opt-in", "multi-layered access"). Social network operators should refrain from collecting and processing data from non-members (such as e-mail addresses or biometric data) and employ data protection-friendly privacy settings and privacy-friendly network software. Users should only be able to publish content about third parties with the latter’s consent.

---

[39] Some 38% of internet users in Switzerland refrain from publishing personal information on social networks. See the Federal Statistical Office's study on "Internet in den Schweizer Haushalten. Ergebnisse der Erhebung Omnibus IKT 2010", p. 47, 85. (only available in German, French and Italian)

The Vorschlag des Konsultativkomitees zur Revision der Europaratskonvention vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Consultative Committee Proposal on the Revision of the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data] (CC 0.235.1) highlights several issues, including that social networks and blogs require special attention[40]. It recommends that users' rights be extended and that data processors equip their services, products and operations in accordance with data protection regulations at the development stage. It also recommends that national data protection authorities be strengthened and that the member states of the Council of Europe give them adequate human, technical and financial support, so that they can carry out their duties independently and efficiently[41].

As part of the reform of the EU 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[42] (which is to lead to a directly applicable regulation in EU countries), various regulations are to be put into place to improve users' control over their data. The proposed standards include strict consent requirements for specified purposes in data processing, as well as comprehensive information and access duties with special consideration of the position of children. The draft regulation envisages data protection through technology, privacy-friendly default settings (privacy by design and privacy by default), the principle of data economy, as well as limits on data storage[43].

#### 4.3.1.2.1 Swiss data protection law in relation to protecting against breach of privacy caused by data processing

The content provided by social network users regularly qualifies as personal data[44] within the meaning of the Federal Act on Data Protection (FADP, CC 235.1). It can often even involve particularly sensitive personal data[45] or personality profiles that enjoy greater protection than ordinary personal data. The Data Protection Act protects natural and legal persons against acts such as those of unlawful breaches of privacy as a result of the processing of personal data by private individuals (Art. 12 FADP). Operators of social networks therefore generally fall within the scope of the law. Since the operators are often based abroad, civil law claims concerning responsibility are often assessed in accordance with international conventions[46] or the provisions of Art. 129ff of the Federal Act on International Private Law[47]. It should also be noted that under federal law[48] the Federal Data Protection and Information Commissioner can only clarify an issue in the case of system faults if the data processing has prominent factors connecting it with Switzerland.

Various violations of the general data protection processing principles (Art. 12 para 2 DSG) are conceivable on social networks. Here are some examples:

---

[40] Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en, p. 4.

[41] Abridged Report of the Consultative Committee of Convention 108, T-PD (2012) RAP 29 Abr_en, p. 22 (Art. 5), 24ff. (Art. 7, $7^{bis}$, 8, $8^{bis}$), 29 (Art. $12^{bis}$).

[42] 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, p. 31

[43] Art. 6 para. 1 lit. a, Art. 7, 11, 14, 15, 23 Proposal for a European General Data Protection Regulation, COM (2012)11 final; see for example Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, p. 60ff

[44] According to Art. 3 lit. a FADP, personal data is any information relating to an identified or identifiable person. According to the Decision of the Swiss Federal Supreme Court 138 II 346 E. 6.1., even if they are not clearly identifiable by the data alone, a person is identifiable if they can be identified from the circumstances, the context of information or on the basis of additional information (e.g. if the owner can be identified via information relating to property).

[45] According to Art. 3 lit. c FADP data on religious, philosophical, political and trade union activities and views on health, privacy or race, social security measures, administrative and criminal prosecution and sanctions is sensitive.

[46] E.G. Lugano Convention of 30 October 2007 concerning the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention), CC 0.275.12.

[47] SR 272; IPRG.

[48] Cf. Decision of the Swiss Federal Supreme Court 138 II 346 E. 3.

- If the operator of a social network does not provide information during the collection of data that it will sell this data to third parties so that they can use them for marketing purposes, or if it does not make clear that it will evaluate the data for advertising purposes itself, this usually constitutes a violation of the principles of the purpose (Art. 4 para. 3 FADP) and detectability (Art. 4 para. 4 FADP) of data processing. If the operator of a social network passes on data to third parties, the latter are also bound to process the data according to the purpose specified during collection of the data[49]; moreover, the disclosure of sensitive personal data and personality profiles to third parties without justification is unlawful (Art. 12 para. 2, lit. c FADP).

- The principles of proportionality and purpose of data processing (Art. 4 para. 2 and para. 3 FADP) can be violated if operators of social networks collect, process and store more data than is necessary for the specified purposes of processing them. Moreover, the principle of proportionality for data processing appears important if sensitive personal data (e.g. regarding race, privacy or religious and political views; Art. 3 lit. c FADP) is used for marketing purposes.

- If social network data becomes the subject of data theft or data leaks because the platform operator has not complied with reasonable technical and organisational protection measures, this usually constitutes a breach of the principle of data security (Art. 7 para. 1 FADP). In relation to data leaks and data theft[50] it is possible to derive a duty to inform on the part of the platform operator from the principle of data security and the principle of good faith (Art. 4, para 2 FADP).

- Users are also bound by the data processing principles. If, for example, they upload contacts from phone and e-mail address lists or instant messenger services to a social platform, the principles of purpose and recognition (Art. 4 para. 3 and 4 FADP) stipulate that the platform operator and publisher of the contact details must inform the data subject of this data collection and its purpose, unless this is apparent from the circumstances.

- The FADP does not provide for specific protection of children. However, in the case of processing the personal data of children, compliance with certain processing principles, such as the principle of recognition or of the principle of good faith, will require more diligence than is usual in the processing of personal data of adults.

#### 4.3.1.3 Justification – specific consent to data processing

Data processing that infringes personality rights may be justified by an overriding private or public interest, by law, or the consent of the person whose rights have been infringed (Art. 13 para. 1 FADP). Although the Federal Supreme Court has ruled that it is not entirely impossible to justify processing personal data in contravention of the general data processing principles, grounds for such justification can only be approved in specific cases with considerable restraint[51].

In the case of the processing of data by platform operators, the justification of the consent of the data subject is the primary consideration. In order to be able to use the services of social networks, users usually provide a declaration of consent in relation to data protection regulations in the General Terms & Conditions (T&Cs). In so doing they agree in principle to the data processing described by the operator in the T&Cs. However, it is possible to question the validity and extent of this consent.

Problems can arise when the power of judgement (Art. 16 CC) of a person is doubtful with regard to the content of the contract, for example, in the case of *children* who disclose personal information about themselves. Children incapable of exercising judgement are represented by their parents within the scope of parental care. It is assumed that the parents can in principle give their consent to certain

---

[49] BSK-DSG, Maurer-Lambrou Urs/Steiner Andrea, 2nd ed., Basel 2006, Art. 4, p. 83 margin number 16.

[50] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 82 no. 16.

[51] See Decision of the Swiss Federal Supreme Court 138 II 346 E. 7.2 with reference to Decision of the Swiss Federal Supreme Court 136 II 508 E. 5.2.4.

types of data processing on behalf of the child in question (e.g. the publication of the photo of a toddler on a social network[52]).

Children capable of exercising judgement can indeed act independently if it is a matter of personal rights (Art. 19c para. 2 of the Civil Code) or personality rights affected by the processing of their personal data. In principle, they may disclose information about themselves under privacy law without parental consent (for details, see Section 4.6.1.3). For the consent of a child capable of exercising judgement to be valid in data processing which infringes privacy, the data processor should however formulate and present the necessary information in such a way that they can understand and comprehend this.

Moreover, in view of the frequently changing uses of user data, and the sometimes difficult nature of comprehending privacy policies and the questionable clarity regarding the consequences of certain data processing, there may also be limits to consent in terms of content.

When entering into a contractual relationship, users often forgo reading the General T&Cs due to their typical length and the style of language. If a data protection declaration of consent has been added to the T&Cs and users do not read the latter upon conclusion of contract (global adoption), their consent to unusual clauses unrelated to the designated business purpose will essentially not be effective unless they have been specifically advised of their existence[53]. In the event of doubt, ambiguous clauses in the T&Cs are to be interpreted against the party offering them. If the interpretation of the conditions of use does not produce any clear conclusion, it is to be interpreted in the sense most favourable to the user.

Consent to data processing that infringes personality rights exists only if it is valid and has not been revoked[54]. Consent is valid only if it has been granted prior to processing, on the basis of adequate information and voluntarily (i.e. without deception, threatening behaviour or coercion)[55]; in the case of handling of sensitive personal data or personality profiles, the giving of consent must also be made expressly clear (Art. 4 para. 5 FADP). In the case of social networks, the form and content of user information play a particular role in this context. This should be clear, factual, accurate, easily accessible, easily recognisable and not misleading[56].

If ordinary personal data is processed, consent may be implied or arise from the behaviour of the data subject, for example, if this person makes their data accessible on a social network[57]. However, the more sensitive the personal data to be processed is, the clearer the consent must be[58]. On the internet, a mouse click should be all that is required to confirm a declaration of consent in relation to data protection; this is the case for the use of most social networks that satisfy the requirements of express consent[59].

If users consent to the conditions of use of social networks, they accept – provided that they have been adequately informed – the practical operation of the service, and in so doing, for example, that

---

[52] For the human rights issues of such recordings cf. the facts of ECtHR Judgement "Reklos & Davourlis vs. Greece" (Case no. 1234/05) of 15.01.2009.

[53] BSK-DSG, Maurer-Lambrou Urs/Steiner Andrea, 2nd ed., Basel 2006, Art. 13, p. 194 margin number 13 and Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 112 no. 90.

[54] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 386 no. 3.

[55] The following are extremely critical of Facebook's privacy policy: Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010 p. 56, 59 and Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013/2, p. 63f.

[56] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 106 no. 75.

[57] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 108 no. 79.

[58] BBl 2003 2127f.

[59] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 108 no. 78.

third parties publish content about them and on their profile without prior consent. Insofar as the activities of third parties do not violate applicable law (e.g. in the form of defamation, violations of the right to their own image or word, breaches of professional confidentiality etc.), there is little users can do against this. One reaction that might be considered would be for users to forego membership in social networks with such open forms of communication or to delete objectionable content on their profiles. However, in cases of content that is of considerable interest to the networking community, deletion is only of limited use if this content has already been copied or linked several times.

#### 4.3.1.4 Generally accessible personal data

Personal data is generally accessible if an undetermined number of people can retrieve it without significant obstacles. If social network users provide data about themselves, there is generally no infringement of personality rights as long as the data has been made generally accessible with their knowledge and consent and processing has not been explicitly prohibited (Art. 12 para 3 FADP). This also applies to the cross-border disclosure of personal data to countries with inadequate levels of data protection (Art. 6 para. 2 f FADP).

In principle, users can make their own decisions regarding the accessibility of information on the basis of the settings offered. In most social networks, various forms of communication are available with different levels of privacy; this makes everything from individual to mass communication possible. If users are adequately informed of the various possible forms of communication and their privacy, it is possible, based on their choice of the form of communication, to estimate whether private communication was intended or the information was made generally available.

Processing of personal data that is made generally accessible may constitute an infringement of personality rights if the data is processed for purposes for which, in the circumstances and when considered objectively, it was not made generally available[60]. This is particularly relevant to data that is made generally accessible on the internet because of the ease with which it can be found[61]. If a person makes their photos available to the public on a social network, anyone may view them in principle, but unauthorised use of images for corporate advertising campaigns are not permitted. The use of such images is also problematic in the framework of conventional journalistic media coverage.[62]

In this context, the question of whether the unsolicited downloading and storing of content from other user profiles is still covered by the purpose of publication has to be considered anew for each individual case. In each case other network members and the platform operator must also adhere to the processing principles of the Data Protection Act.

#### 4.3.1.5 Special issue of the transfer of all rights of use to the platform operator

If the unlimited storage and use of any content published on social networks by users expressly becomes a subject of the contract between the user and platform operators, the question arises as to whether a contract with this content is valid. It cannot be ruled out that such a contract could in certain cases qualify as a transaction that infringes personality rights (Art. 19 para. 2 and Art. 20 para. 1 of the Code of Obligations); Art. 27 para. 2 CC), especially as data published on social networks and subsequently linked data is often sensitive or constitutes a personality profile, while the relationship between performance and consideration raises questions (a communication infrastructure offered by the plat-

---

[60] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 381 no. 76.

[61] BSK-DSG, Rampini Corrado, 2nd ed., Basel 2006, Art. 12, p. 187 margin number 18.

[62] As an organ of institutionalised self-regulation in journalism, the Schweizer Presserat (Swiss Press Council) has reminded journalists to exercise restraint in of the use of information regarding private individuals published on the internet several times. Anyone who publishes images on a blog or other publicly accessible platform does not simply agree to subsequent processing in other media. Those working in the media sector must carefully balance the protection of privacy with the public interest; see, for example Swiss Press Council Opinion no. 43/2010 of 1 September 2010: Internet and privacy; www.presserat.ch/ 28340.htm (Only available in German, French and Italian)

form operator versus transferring extensive rights to users' personal data)[63]. In this context, however, users have a significant influence on what parts of their data are published on social networks.

#### 4.3.1.6 Other protection instruments of the Swiss legal system

In addition to the Data Protection Act, the Swiss legal system has other tools to protect against non-transparent methods of acquiring, processing and disclosing data by social network operators. For example, the possibility of **rescission of contract** under private law may be considered in the event of fundamental error (Art. 23ff. of the Code of Obligations) or fraud (Art. 28 of the Code of Obligations)[64].

Moreover, the use of unfair General Terms & Conditions (T&Cs) constitutes an unfair business practice (Art. 8 of the Federal Act of 19 December 1986 on Unfair Competition (**UCA**), CC 241). With the latest amendment of the UCA, since 1 July 2012 every use of T&Cs that violates the principle of good faith has been deemed unfair if it causes a significant and unjustified imbalance between contractual rights and obligations to the detriment of its customers[65]. The new version annulled the previously existing requirement of deception (proof of the risk of deception) in Art. 8 UCA, which means that open content control of the T&Cs is now possible for the consumer market.[66] With regard to the T&Cs of social media providers, the question arises of whether clauses before the new Art. 8 UCA, which allow unilateral adjustment of T&Cs by the platform operator without notice or informing customers in person, would stand up.

Moreover, the repeated unjustified violation of the processing principles of the Data Protection Act could be unfair within the meaning of the general clause of Art. 2 UCA, if the data processor is able to gain competitive advantage over its competitors by violating the FADP[67]. Possible examples include personal data that is acquired, processed and sold for advertising purposes in violation of data protection law.

#### 4.3.1.7 Assessment

Overall, it can be stated that existing Swiss law, with its openly formulated protection rules, allows relatively extensive protection against the typically problematic data processing on social networks. There are, however, various identifiable difficulties that hinder efficient data protection and are also relevant to social networks. They lie, for example, in the frequently insufficient recognition of problematic data processing, the tremendous increase of data processing in an international context (which makes identification and implementation much more difficult; cf. Chapter 5) and the relatively low probability of sanctions. In addition there is the fact that users are rarely aware of their legal rights and that given the large number of relevant facts, the FDPIC is at the limit of its resources[68].

There is potential for improvement, for example, via privacy-friendly default settings (*privacy by design* and *privacy by default*) as well as clearer formulation of privacy policies. In the evaluation report on the FADP, the Federal Council has announced that it will extend the concept of privacy by design by the promotion of privacy-friendly technologies and measures to improve the control and ownership of data.[69]

---

[63] Schwenzer Ingeborg, Schweizerisches Obligationenrecht Allgemeiner Teil, 6th ed., Bern 2012, p. 256f.

[64] As regards the legal remedy cf. Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, digma 2001 p. 108, 111-114.

[65] AS 2011 4910.

[66] The legislature intended to prepare the way for open content control by deleting the offence of deception (Federal Gazette 2009 6178).

[67] Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zurich 2011, p. 65f.

[68] Federal Council Report concerning the evaluation of the Federal Act on Data Protection of 09.12.2011 (BBl 2012 341-345, 349).

[69] Report concerning the evaluation of the Federal Act on Data Protection of 09.12.2011, no. 5.2.2 (BBl 2012 350).

### 4.3.2 Creating and administrating comprehensive user profiles (data mining)

#### 4.3.2.1 Background

Users provide comprehensive information about themselves for purpose of registration as well as through their activities on social networks and the metadata associated with internet use (connection time, approximate geographical origin of the IP address, residence time and movements on the web-site etc.). For example, the placement of Facebook "like" buttons on third-party websites allows Facebook to obtain information about the visitors to the website.

In the case of many platform operators it is unclear how the collected data will be used. Merging all the information that results from the use of social networks can lead to the creation of meaningful but also error-prone profiles. If the platform operator sells data packages to third parties, the profiles can be used as a basis for offering good and services. This is problematic not only because of the economic exploitation of the data, but also because of the potential for discrimination.

#### 4.3.2.2 Solutions in other countries and in international law

The Recommendation of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of profiling[70] deals with the observation, collection and matching of personal data on the internet and requires extensive rights for data subjects. Social networks are an important source for such data processing. The Council of Europe has identified the lack of transparency of profiling, the potential for discrimination against data subjects and the insufficient protection of children from such data collection as problematic. It also calls for access to goods and services (and information about these) to be made possible without having to provide data that is not necessary for the provision of services or delivery of goods. In addition, it suggests that providers of information society services should also ensure that information regarding their services is available without the need to create a profile.

Art. 20 of the Proposal for an EU General Data Protection Regulation[71] intends to protect (subject to certain exceptions) natural persons from automated processing of their data with the aim of analysing or predicting certain characteristics regarding their person or situation in life. The requirement for protection is that the processing affects the data subject in a significant manner or produces legal effects with regard to them. If personal data is processed to operate direct marketing, data subjects are, under Art. 19 para. 2 of the proposal, given the right to appeal free of charge.

The US agency for consumer protection and competition law, the Federal Trade Commission (FTC), has asked the internet industry to establish a "do-not-track" option. This should allow consumers to decide which information will be shared about their online activities, as well as with whom and for what purpose (the emphasis here is on direct marketing measures)[72].

The Transatlantic Consumer Dialogue (TACD)[73] has issued a resolution on social networking[74]. This calls for the enactment of laws stipulating that social networks do not make access to their services dependent on the consent of the user for their data to be used for marketing purposes. In addition, it

---

[70] Recommendation CM/Rec(2010)13.

[71] Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final).

[72] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, FTC Report March 2012; available at: http://www.ftc.gov/opa/2012/03/privacyframework.shtm . The report on the protection of consumer privacy on the internet contains recommended guidelines for the internet industry. This calls for companies to develop their internet services in such a way that a high level of privacy protection is automatically provided (privacy by design) and consumers are fully informed about the purpose, scope and type of data used.

[73] The TACD is a forum for US and European consumer associations that develops consumer protection recommendations for the US government and the European Union, see: http://www.tacd.org/.

[74] Resolution on Social Networking of May 2010, Doc no. Infosoc 43-09; available at: http://tacd.org/index.php?option=com_docman&task=cat_view&gid=83&Itemid=40.

believes that the explicit consent of users should be mandatory in the case of data collection for marketing purposes and that children under 16 years of age and websites that are primarily visited by children of this age should be fundamentally excluded from advertising measures.

#### 4.3.2.3 Legal status in Switzerland

The collection and collation of data resulting from user activity in many cases leads to the creation of personality profiles within the meaning of Art. 3 lit. d FADP. The Data Protection Act places special demands on the processing of personality profiles (Art. 4 para. 5, Art. 11a para. 3 lit. a, Art. 12 para. 2 lit. c, Art. 14 FADP).

If platform operators create personality profiles using data linkage, this may violate the principle of good faith due to insufficient visibility of this linkage (Art. 4 para 2 FADP). Moreover, in this instance the obligation of the holder of the data file to provide information to the data subject comes into effect upon procurement of the personality profile (Art. 14 FADP). The transfer of user data to Facebook by embedding the "like" button on third party websites may violate the principle of recognition (Art. 4 para. 4 FADP) due to a lack of awareness on the part of website visitors about the data transmission that takes place. Moreover, the provision of very general processing purposes at the time of data collection, e.g. the creation and processing of user profiles "for marketing purposes", may not be sufficient as regards the principle of purpose limitation (Art. 4 para. 3 FADP). At the time of data collection users are often insufficiently aware of the purpose that their user profiles will be used for later.

The collection of a variety of personal data and compiling it to create personality profiles could also be in conflict with the principle of proportionality for data processing (Art. 4 para. 2 FADP). Moreover, the principle of data accuracy (Art. 5 FADP) may be involved in connection with the creation of personality profiles: the automated collection, collation and evaluation of data leads to the loss of the original context in which the data was created and may result in false statements[75].

It is particularly relevant that in the case of personality profiles the consent of the data subject must be explicit (Art. 4 para. 5 FADP). This increases the demands on the information regarding the creation, use and disclosure of personality profiles, especially if they are included in the T&Cs. The explicit nature of consent might, for example, be doubtful if certain unusual processing purposes or disclosure to third parties are not emphasised. Explicit consent is required if the processing of personality profiles is contrary to the principles of processing or if disclosing of personality profiles to third parties is to be justified by means of the consent of the data subject (Art. 13 para. 1 in conjunction with Art. 4 para. 5 FADP). In the context of social networks this is of particular importance because their business models are usually based on the sale of user profiles, which can be classified as disclosure of data to third parties.

The FADP does not recognise specific protection of children from the creation and processing of data. Here, however, the specifics of the consent to the processing of the personal data of a child should again be taken into account (see Section 4.3.1.3.). There is also no fundamental prohibition to undertake advertising activities with regard to children under the age of 16 or on websites oriented to children of this age.

The principle of **telecommunications confidentiality** in Art. 43 TCA and Art. 321$^{ter}$ SCC protects the confidentiality of telecommunications. However, it cannot as a rule protect against the creation of personality profiles. Only in exceptional cases where platform operators transmit information between several users, would the principle of telecommunications confidentiality protect these users' telecommunications data from being transmitted to third parties and used to create user profiles.

---

[75] Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 p. 108, 109.

### 4.3.3 Lack of a right to be forgotten

#### 4.3.3.1 Background

The lack of control users have over their data on social networks is also manifested in the difficulty of irrevocably deleting user accounts. Deregistering an account usually only covers the deactivation of the profile; the data continues to be stored on the platform operator's server. Permanent deletion of all content is often, but not always, possible. The process can also prove to be very complicated, which means that users are deterred by, or cannot understand it. Moreover, active users can leave large amounts of information and content on other network pages and profiles. Comprehensive deletion is in practice almost impossible.

The benefit of a potential cancellation of the original profile is also diminished by the fact that on certain platforms it is possible to download and save data from third-party user profiles. This can lead to a myriad of private data collections. Even if users delete their original profile, their data can remain stored in another location. It is now also possible for third parties to archive data in other ways (e.g. using screenshots) and republish this at a later date.

#### 4.3.3.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services and the Proposal for an EU General Data Protection Regulation[76] provide under certain conditions for the right to be forgotten, the deletion of personal data and the elimination of any other data dissemination.[77] In particular, they provide for the right of children to be forgotten and data deletion[78].

The Draft amendment to the German Telemedia Act also provides for a right to deletion of user accounts on social networks and all the content generated by users[79].

#### 4.3.3.3 Legal status in Switzerland

In principle, the right to be forgotten on social networks means the right of users to deletion of the content that they have published on social networks. The right to deletion can be derived from the Data Protection Act and the protection of personality under civil law.

The **right to data protection** prohibits the processing of personal data against a person's express wishes (Art.12 para. 2 b FADP). Since the storage and archiving of personal data may be the subject of an express prohibition on processing, it may be possible to demand comprehensive or partial deletion of personal data using the right of objection[80]. Consent in accordance with Art. 13 para. 1 FADP, by means of which data processing that infringes personality rights is justified, can in principle also be revoked. However, the revocation is effective only for the future, not for completed data processing[81]. Therefore if perpetual storage of data has been agreed, this consent may in principle be revoked for future data storage.

If third parties violate the processing principles of the Data Protection Act without justification, a right to delete the data concerned may arise from Art. 15 para. 1 FADP. Possible examples include cases in which other users publish the personal data of data subjects on social networks without it being evident to the data subject (Art. 4 para. 2 and 4 FADP). It is also possible that they have disclosed sensi-

---

[76] Art. 17 Proposal for an EU General Data Protection Regulation, COM (2012) 11 final.

[77] cf. Treyer Tobias, Das "Recht auf Vergessen" im digitalen Zeitalter, in medialex 2013, p. 61f.

[78] Art. 17 para. 1 of the Proposal for an EU General Data Protection Regulation, COM(2012)11 final. cf. the Declaration of the Council of Europe on protecting the dignity, security and privacy of children using the internet.

[79] Draft amendment to the German Telemedia Act, 17/6765.

[80] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 362 no. 32.

[81] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 118ff. no. 104ff.

tive personal data or personality profiles of a person to other network members or third parties without justification (Art. 12 para. 2 c FADP), process the personal data of a person for a purpose other than that indicated at the time of collection (e.g. by reusing statements made in a particular forum or on a specific topic within a social network in a context with a different purpose)[82] or process personal data against the express will of the data subject (Art. 12 para. 2 b FADP).

Arguments for a right to deletion also arise from the **protection of personality under civil law** (Art. 28 CC); however, this depends on balancing the interests at stake, or on the question of whether there are grounds for lifting the illegality of infringing personality rights. Art. 28 CC comprises various sub-levels. The right to be forgotten can be asserted by invoking the protection of moral integrity, privacy, honour or the right to one's own image, name or word. Art. 28 CC prohibits third parties from collecting or publishing content from the secret or private domain or photos of a person without their consent to procure (or other valid justifications). Art. 28a para. 1 lit. 2 CC gives the data subject the right to remove an existing violation, which in principle also entails the deletion of content on the internet that violates personal rights. If users publish content about themselves on social networks and this is then processed by a third party, it should be noted that consent given for a particular purpose does not include other uses[83]. Under civil law, it is problematic for example, if statements made by a person are used for false quotes[84], published photos of a person are used in a different context or purpose without their consent[85], or if a person's name is used in a way that violates their personality rights[86]. It is also to be assumed that consent that is given once can be revoked, but the existence of a right to deletion also depends on the outcome of balancing specific interests[87].

The form in which the data subject has published content (private or public communication?), the nature of this content (is it in the secret, private or public domain?) and what type of person the data subject is also plays a role in any right to deletion. If a data subject has made content generally accessible (within the meaning of Art. 12 para. 3 FADP), then this circumstance will, as part of balancing specific interests with regard to any right of deletion they assert, have to be taken into account in favour of the platform operator (Art. 13 para. 1 FADP; Art. 28 para. 2 CC). However, the more relevant the data is to the personality of the data subject, the more the interest of the data subject in the deletion of their data will have to be taken into consideration, even if they have published this at another time themselves. If the data subject is an absolute or relative figure of contemporary history[88] or an official, then a legitimate public interest may prevent deletion of content. However, after an appropriate amount of time has passed, a right to be forgotten could be revived[89]. If personal data that was published while the data subject was a child are deleted, then interference in their personality rights due to the special need for protection of children and children's partially limited ability to understand is in principle more likely to be approved than when it relates to data belonging to adults.

---

[82] This could affect the principles of purpose and accuracy of the data (Art. 4 para. 3 and 5 FADP).

[83] BSK-DSG, Meili Andreas, 4th ed., Basel 2010, Art. 28, p. 269 margin number 48.

[84] Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: medialex 2011 p. 197, 199.

[85] BSK-ZGB I, Andreas Meili, 4th ed., Basel 2010, Art 28, p 260 margin number 20, which indicates that in practice, digital and conventional retouched images, photomontages and actual image manipulations, and the use of archived images in a completely different context than when the photograph was originally taken often lead to problems.

[86] BSK-DSG, Meili Andreas, 4th ed., Basel 2010, Art. 28, p. 320 margin number 1.

[87] BSK-DSG, Meili Andreas, 4th ed., Basel 2010, Art. 28, p. 259 margin number 48.

[88] Athletes, politicians, artists, business leaders and other prominent persons are absolute figures of contemporary history; relative figures of contemporary history are persons who draw public interest as the result of a specific event. See BSK-DSG, Meili Andreas, 4th ed., Basel 2010, Art. 28, p. 271 margin number 52.

[89] See e.g. Decision of the Swiss Federal Supreme Court 109 II 353 E. 3 and BSK-DSG I, Meili Andreas, 4th ed., Basel 2010, Art. 28, p. 271 margin number 52.

Another problem that concerns the right to be forgotten is the digital assets and the handling of data left on the internet by the deceased. The law of persons, inheritance law and data protection law provide only an incomplete solution[90].

The analysis indicates that to some extent the existing legislation guarantees the right to be forgotten; however, due to conflicting interests (e.g. information in the public interest, the proportionality of measures imposed on platform operators, etc.) this is in principle reasonably limited by conflicting interests[91].

Despite the presence of certain legal options to remove certain content, it may prove to be very complicated to effect comprehensive deletion on social networks. This problem comes to a head when large numbers of third parties have already downloaded or made further use of the content concerned.

In an evaluation report on the FADP, the Federal Council is giving consideration to clarification of the right to be forgotten.[92]

### 4.3.4 Searchability of user profile data in search engines

#### 4.3.4.1 Background

Using metadata, which are incorporated into Web pages, search engine robots can be prompted not to include certain content and pages in their index or cache. Operators of social networks can design search engine data access accordingly. Social networks that withdraw the decision-making power from users as to whether the data provided by them on the social network can be retrieved by internal or external search engines are problematic.

#### 4.3.4.2 Solutions in other countries and in international law

The Council of Europe Recommendation on the protection of human rights with regard to search engines[93] calls for users to be given the right to request search engine operators to immediately delete their personal data if copies of the original websites that have already been erased continue to be stored by search engines. Moreover it calls for users to be given the right to request search engine operators to delete and correct the data processed about them. The Council of Europe Recommendation on social networking services calls for users to be allowed to make an informed decision about the indexing of their data and the right to delete their data on search engine caches.

The Draft amendment to the German Telemedia Act requires that user accounts and user-generated content only be retrievable on search engines with the prior consent of the user[94].

#### 4.3.4.3 Legal status in Switzerland

If social networks allow search engines to access the personal information of network members, this constitutes a disclosure of data within the meaning of the Data Protection Act (Art. 3 lit. e and f FADP), to which data processing principles are applicable. The principle of visibility of data collection (Art. 4 para. 4 FAPD) allows the data subject the right to be informed of the access search engines have to their personal data that has been published on social networks, unless this is apparent from the circumstances.

---

[90] Comprehensive information on this subject can be found in Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012.

[91] According to European Court of Human Rights jurisprudence, the ECtHR is not permitted to grant rights to deletion of illegal media publications from online archives to those affected. It is not a task of the judiciary to eliminate all traces of illegal content: ECtHR Judgement "Wegrzynowski & Smolczewski vs. Poland" (no. 33846/07) of 16.7.2013, para. 65.

[92] Report concerning the evaluation of the Federal Act on Data Protection of 09.12.2011, no. 5.2.2 (BBl 2012 350).

[93] Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines.

[94] Draft amendment to the German Telemedia Act, 17/6765.

Given the large amount of data published on social networks and the often highly personal nature of it, it is likely that there will be many cases of sensitive personal data and personality profiles. Due to the absence of other justifications (Art. 13 para. 1 FADP), express permission (Art. 4 para. 5 FADP) will in the overwhelming majority of cases be required in order for search engines to be able to access user data. It follows from the principle of purpose limitation that third parties (in this case search engine operators) are strictly bound to the purpose of processing applicable at the time the data was collected[95].

If search engine operators ignore the restrictive information social network operators provide to search robots with regard to the accessibility of user data and if they continue to collect and make the data publicly available, this practice could, due to its clandestine nature,[96] qualify as unlawful (Art. 4 para. 1 FADP) or as illegal data collection.

### 4.3.5 Problems of image recognition

#### 4.3.5.1 Background

Photos uploaded to social networks with identifiable individuals and their associated user profiles can serve to develop and improve facial recognition software. This software can compare people on photos that are published later with the collected data and match to a user profile. If third parties upload images to a platform that feature other network members, this type of software can suggest the connection of those depicted with a registered profile (tag suggest)[97]. Moreover, facial recognition software can identify people interested in anonymity (e.g., on a dating website) or connect them to their CV on a company website using the photos on the social platform and the associated name.

Similarly, automatic recognition of other information contained in images is based on outlines, colours, or the surface structure of the objects shown (content-based image retrieval). This function can identify specific objects or buildings and possibly provide the geographic location of a scene, which could lead to the disclosure of addresses, stalking or other harmful or illegal acts.

#### 4.3.5.2 Solutions in other countries and in international law

Facebook suspended the use of its facial recognition software in the European Union in compliance with the requirements of the Irish Data Protection Commissioner[98]. The compromise was partly the result of a general review of the compatibility of the company's services and the data protection laws of Ireland and the European Union. According to the FDPIC the agreement also applies to Switzerland.

The Council of Europe Recommendation on social networking services requires that technologies that have a significant impact in the private domain of users (e.g. those based on the processing of sensitive or biometric data such as facial recognition software), should guarantee increased data protection and not be used without the consent of the user.

In an Opinion on facial recognition in online and mobile services[99], the Article 29 Data Protection Working Party, an independent advisory body to the European Commission, dealt with the data pro-

---

[95] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 95 no. 47.

[96] Clandestine data collection fundamentally violates the principles of good faith and the visibility of data processing (Art. 4 para. 2 and 4 FADP).

[97] For example, person A examines the photos taken by person B using an image recognition program, recognises person C and names them on the photo.

[98] Report of Re-Audit Facebook Ireland Ltd of the Data Protection Commissioner from 21.09.2012; available at: http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f; Driessen Benedikt / Dürmuth Markus, Anonymität und Gesichtserkennung, in: digma 2013, p. 54

[99] Art. 29 FADP Opinion 00727/12/DE WP 192.

tection risks of this technology and issued recommendations to data processors on obtaining the valid consent of the data subject as well as encryption of transmitted data and its safekeeping.

#### 4.3.5.3 Legal status in Switzerland

Facial recognition software on social networks can only be applied once photos have been posted on such a platform. Part of Art. 28 para. 1 CC, protects the individual's right to their own image against the illegal use of their own image[100]. In principle, no-one can be depicted and existing photographs may not be published without prior or subsequent consent; moreover, the consent to take the photograph is not the consent to any conceivable subsequent publication, but strictly applies only to that obvious to the data subject when the photograph was originally taken[101].

Data protection law too, whose private-law provisions supplement and substantiate the protection of personality[102], ensures that no images of a person[103] are published without their knowledge. The principle of the visibility of data collection (Art. 4 para. 4 FADP) requires that it is apparent to the person portrayed, at least from the circumstances, when images of them are published on social networks. Moreover, the principle of purpose guarantees that personal data is processed only for the purpose that was clearly stated when the photograph was taken. The publication of photos of a person on social networks in the absence of justification (Art. 13 para. 1 FADP) is therefore only permissible if it was evident when the photograph was taken that it would be published on a social network.

If photos of persons are published on social networks, their analysis and combination with user profiles through facial recognition software is only permitted if the data subject has been informed of this form of use[104]; this is by no means true of photos published by third parties without the consent of the data subject. Photographs will regularly qualify as sensitive personal data (Art. 3 lit. c FADP), which will result in correspondingly stricter data protection requirements[105]. In principle, the use of automatic facial recognition software and the "tag suggest" function may also violate the principle of proportionality of data processing (Art. 4 para. 2 FADP).

The question is how to categorise a situation in which a person knowingly and willingly publishes their own photos on a social network and makes their profile generally accessible by means of user settings (Art. 12 para. 3 FADP). If personal data that is made generally accessible is processed for purposes for which, in the circumstances and when considered objectively, it was not made generally available, this may nevertheless constitute an infringement of personality rights[106]. Given the relative novelty of the use of facial recognition software, doubts may exist as to whether a person who makes their photos generally accessible, has also published them for the purpose of such processing. In this case too, the existence of consent to the specific processing would have to be examined[107].

As for the automatic recognition of features and objects in images by software programs, this information should be classified as factual data. Factual data is always personal data within the meaning of

---

[100] Bächli Marc, Das Recht am eigenen Bild, Basel 2002, p. 69.

[101] This is unless there is a justification within the meaning of Art. 28 para. 2 CC. A barrier to the right to one's own image is the legitimate right to publish (freedom of expression in accordance with Article 10 of the Convention); cf. the corresponding Strasbourg legal practice Zeller Franz, Das eigene Bild und sein begrenzter Schutz [one's own image and its limited protection], in: digma 2013/2, p. 50ff

[102] Schweizer Michael, Recht am Wort, Bern 2012, p. 209.

[103] The term "personal data" in the Data Protection Act also includes images of persons if these can be assigned to a person; consequently it also includes photographs.

[104] This follows from the requirement for consent in accordance with Art. 28 para. 2 CC and Art. 13 para. 1 FADP and from the principles of good faith and purpose of the data processing in accordance with Art. 4 para. 2 and 3 FADP.

[105] See Art. 4 para. 5, Art. 11a para. 3 lit. a, Art. 12 para. 2 lit. c and Art. 14 FADP.

[106] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 381 no. 76.

[107] Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 383 no. 84.

the Data Protection Act if it can be associated with a person. Property and motor vehicles are examples of this[108]. In this case, they also enjoy protection under data protection law.

### 4.3.6 Problems of geolocation (location technology)

#### 4.3.6.1 Background

Certain social networks offer services that use positioning technologies such as GPS or WiFi to locate and provide users (whose data are usually transmitted via smartphones) with their desired geographic information. Some social networks are entirely dedicated to such geolocation services[109]. Depending on users' communication behaviour, platform operators can connect a variety of data to the spatial data collected. This means in certain circumstances that platform operators may know not only the approximate location of users, but possibly even which building they are in (e.g. theatre, restaurant, etc.), with whom, what they are doing or even how they are feeling.

The connection of these positioning services with social networks can lead to users consciously or unconsciously communicating information about their whereabouts and activities there, which third parties can use for purposes not intended by the user. Harmful behaviour such as identity theft, cyberbullying, cyberstalking and cybergrooming can be facilitated by such technologies. Moreover, geographic data can inform third parties of where the data subject is and where they live, thus making it easier to commit burglary[110].

#### 4.3.6.2 Solutions in other countries and in international law

The Article 29 Data Protection Working Party[111] has dealt with the data protection risks of geolocation services in an Opinion of May 2011[112]. The central theme is user consent, which according to the opinion is invalid if it is based on the mandatory acceptance of T&Cs or exclusively on the option to "opt-out". It recommends that geolocation services always be turned off with the option for users to "opt-in" and that users should be made explicitly aware of unusual processing purposes, for example, the creation of profiles or behavioural targeting. It suggests that if users are informed about changes in the processing purpose and data transmission, their silence should not be interpreted as consent. It recommends that terminals notify users when geolocation services are in operation via a warning symbol and that service providers regularly re-seek user consent without changes to service. It also recommends that the retention period should be appropriately short and that users should have the right to information in a readable format as well as the right to amend or delete their data.

#### 4.3.6.3 Legal status in Switzerland

Within the meaning of the Data Protection Act, geodata is personal data if a link to a natural or legal person exists or can be made with reasonable effort[113]. Moreover, locating mobile devices associated with persons and linking factual and personal data may result in personality profiles or sensitive personal data[114], which are subject strict requirements according to data protection law. The data protection risks of the geolocation services used by social networks are in principle recognised by the processing principles of the Data Protection Act.

---

[108] BSK-DSG, Belser Urs, 2nd ed., Basel 2006, Art. 3, p. 64 margin number 5. Within this meaning see also Decision of the Swiss Federal Supreme Court 138 II 346 E. 6.2.

[109] cf. Foursquare (https://foursquare.com/) and Friendticker (http://en.friendticker.com/).

[110] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zurich 2012, p. 162f.

[111] https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/Cooperation/Art29

[112] Opinion 13/2011 on Geolocation services on smart mobile devices of 16.05.2011, 881/11/DE WP 185.

[113] BBl 2006 7851 f.

[114] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zurich 2012, p. 48f., 55f.

For example, the principle of *proportionality* (Art. 4 para. 2 FADP) is applied if more data is collected and linked than is necessary for the processing purpose – the principle of proportionality may even require the anonymisation of geocoded data[115].

The principle of *purpose* (Art. 4 para. 3 FADP) covers amendments to the purpose of processing if due to their usefulness, platform operators retrospectively use the personal data collected for new purposes. The generation of ordinary personal data, personality profiles and sensitive personal data by means of linking geo- and other data published on social networks must be recognisable to the data subject[116] and in the case of data linkage, the operators of social networks must take reasonable precautions to prevent the creation of incorrect data (Art. 5 § 2 FADP).

As with many services offered by social networks, the problem of a lack of awareness on the part of the users of the extent, distribution, nature and purpose of the processing of their geographic data arises, which can also involve doubts about the effectiveness and validity of their *consent*[117].

Art. 45b of the Telecommunications Act (TCA) regulates geolocation for customers of telecommunications service providers. It is permitted in three cases: first, when this is necessary to provide or bill the telecommunication services; second, by the consent of the customer and third, in anonymous form. However, the majority of social media providers are probably (cf. Section 2.4.2.2*) not also telecommunications service providers, which means that Art. 45b is often not applicable.

### 4.3.7 Excessive binding of users to a social network

#### 4.3.7.1 Background

In economics, the "lock-in effect" describes the situation that occurs when large investments in a joint venture with a partner company make it particularly difficult for a company to extricate itself from this joint venture. The partner company may take advantage of this situation to dictate particularly unfavourable conditions for the joint venture.

Social network users can be in a similar situation if they have invested so much time and effort in their presence on a social platform that changing platforms seems unthinkable. The platform can then make the conditions of use less favourable without the users responding and switching to a competing platform.

This may be the case when users save important images, films, music, text, or other data on the platform. It may also be the case that users reach so many people via a platform (for example, on a personal YouTube channel or a blog) that they would only change platform if they could take these contacts with them to another platform.

A change of platform may also be unthinkable if users can only exchange messages with each other via the platform and if without the platform they were to lose their contact information. On the other hand, other users may in this case also desire to be contacted only via the anonymity of the platform and, for example, not reveal their e-mail address to the platform operator. Migration of contacts when changing platforms would not be relevant to the interests of such users. This conflict of interests can, however, be resolved, if when leaving the platform users are given the opportunity to migrate contact details for those users who wish to do so.

---

[115] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zurich 2012, p. 47.

[116] The principles of good faith and visibility of data processing as well as the duty to provide information of the owner of a data collection take effect in the event of acquisition of personal profiles or sensitive personal data (Art. 4 para. 2 and 4, and Art. 14 FADP).

[117] Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zurich 2012, p. 65.

Some platforms offer users migration of stored files. This data portability between different platforms should be made possible as a matter of principle, because only then does the effort expended by users to change platform reduce to a tolerable level.

#### 4.3.7.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for simple data portability to other providers in a standard electronic format.

The Proposal for an EU General Data Protection Regulation also provides for a right to data portability[118]. If personal data is processed electronically in a structured standard electronic format, the data subject should have the right to request a copy of the processed data in structured standard reusable electronic format. If the data subject has made the personal data available themselves, they should have the right to transfer this data to another system in a standard electronic format without hindrance on the part of the data processor.

#### 4.3.7.3 Legal status in Switzerland

Under Swiss law, there is no standard obliging social networks to provide users who leave the platform with the data they have published or stored on the platform. Such a standard could counteract excessive binding of users to certain platforms.

The existing regulation of number portability under telecommunications law serves a similar purpose. It allows customers to retain their telephone number when they change their telephone provider or residential address. Persons who change service provider can take their telephone number to a new provider, thus saving themselves the effort of informing all of their contacts of their new telephone number. They are therefore more willing to switch to a new provider.

However, the market for social networking is still emerging. The tendency to bind users to a particular platform is therefore not as pronounced as in a mature market. Only once a market has matured does retaining existing customers play an important role for the company. Whether this desire to prevent existing customers from switching their provider means that companies will also retain customer data remains to be seen. In practice it is already clear that much of the existing customer data on popular social networks can already be migrated. In view of the existing voluntary offers today, a special duty to release data does not yet appear necessary. This is underlined by the questions which would be raised when implementing this duty: What data can users migrate? Does it include data that has been combined by the operator with other data so as to be more useful (e.g. identification of the user on photos published by third parties)? Does it include data that has been created with programs belonging to the operator? In what format is the data to be provided in?

How this issue will develop in the future is not yet clear. It is therefore advisable to monitor future developments and possibly adopt legislation at a later date (see Section 7.2.4.4).

## 4.4 Impairment of individual interests by third parties

### 4.4.1 Defamation and illegal infringements of personality rights

#### 4.4.1.1 Background

There are also cases of defamatory value judgement and false assertion on social networks[119]. In Switzerland, courts have already ruled on abuse on social networks[120]. Damage to reputation via so-

---

[118] Art. 18 Proposal for an EU General Data Protection Regulation, COM (2012) 11 final.

[119] In its Annual Report 2011, CYCO drew attention to an increase in cases of defamation reported as well as the fact that criminals increasingly use social networks as the instrument to this end. See the Annual Report 2011 by the Cybercrime Coordination Unit Switzerland (CYCO), p. 6.

cial media cannot simply be compared to defamation in the traditional media (e.g. newspapers). Other countries have recognised that online communication via new channels such as blogs and Twitter presents a unique test for the effectiveness of existing legal instruments to protect reputation. [121]

There are now new risks for data subjects, which are difficult to calculate. Control of one's profile is made more difficult due to the fact that on many social networks content can be posted on third-party user profiles without obtaining prior consent. The simple, immediate and unedited transmission of content on social networks and the often pronounced social relevance of their contact groups means that the damage that derogatory value judgements or false assertions by third parties can cause is considerable.

Another example of phenomena that may lead to the reputation of the data subject being damaged is group invitations on Facebook. If a third party is invited to a group by a Facebook friend, they automatically become a member, independent of their consent. Although they are automatically notified of this invitation and can immediately leave the group, depending on the group profile and the identity of the invitees, damage to their reputation may have already arisen.

#### 4.4.1.2 Solutions in other countries and in international law

One possible measure to protect against false public assertions is the right of reply. According to the recommendation of the Council of Europe on the right of reply in the new media environment[122] it should be applicable to all means of communication that serve the periodic transmission of editorially controlled content to the public, regardless of whether it is published online or offline. It recommends that the relevant content should contain a link to the reply if the disputed content remains publicly accessible in electronic archives and the right of reply has been granted.

The European Parliament and the Council of Europe have called on member states to provide for measures to guarantee the right of reply in online media[123]. In its 2011 Report on the implementation of the recommendation, the European Commission noted that the introduction of a right of reply in online media within the EU member states was very inhomogeneous [124] and called for an improvement in the effectiveness of the system.

---

[120] cf. Entscheid des Kreisgerichtes St. Gallen vom 09.05.2011 (Beschimpfung über Facebook) [Decision of the Divisional Court of St. Gallen of 09.05.2011 (Abuse on Facebook)]; http://wifimaku.com/pages/viewpage.action?pageId=5669650 (only available in German)

[121] From modern non-Swiss literature, cf. Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, p. 710ff.; Richardson Megan, Honour in a Time of Twitter, Journal of Media Law 2013, p. 45ff.

[122] Recommendation Rec(2004)16 on the right of reply in the new media environment.

[123] Empfehlung des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste, ABl. L 378, 27.12.2006, p. 72. [Recommendation of the European Parliament and of the Council on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, OJEC L 378, 27.12.2006].

[124] Bericht der Kommission über die Anwendung der Empfehlung des Rates vom 24. September 1998 zum Jugendschutz und zum Schutz der Menschenwürde und der Empfehlung des Europäischen Parlamentes und Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweigs der audiovisuellen Dienst und Online-Informationsdienste – Schutz der Kinder in der digitalen Welt, KOM(2011) 556 endgültig, p. 10 [Report on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity and of the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and online information services industry – Protecting Children in the Digital World, COM(2011) 556 final].

#### 4.4.1.3 Legal status in Switzerland

Protection against defamation under criminal law (Art. 173-178 SCC) and under civil law (Art. 28f. CC) are generally applicable to activities on social networks. Economic protection against defamation (Art. 28 CC) is supplemented by Art. 3 para. lit. a UCA.

The Civil Code recognises as a special instrument the right of reply against assertions in periodical media that are addressed to or accessible by the public (Art. 28g – 28l CC). The legislature has deliberately formulated the concept of the media in an open manner, so the right of reply also applies to new forms of media and does not depend on the transmission technology. [125] Whether a user profile on a social network qualifies as periodical media depends on the specific use of the respective platform or the publication behaviour of the profile owner. It would thus be possible to classify regularly updated journalist blogs as periodical media within the meaning of the CC whilst this is doubtful in the case of discussion forums[126].

The practical problems in proceedings against social network posts that are defamatory or infringe personality rights appear primarily to lie in *law enforcement* if the author of a libel cannot be identified and the investigation depends on the cooperation of platform operators and providers. Prompt action against publications on foreign platforms is particularly difficult.[127] However, if any persons involved in the crime are Swiss, enforcement of the law is facilitated by the fact that deletion and determination requests can be issued against anyone involved in the infringement of personality rights.[128]

Legal instruments are also largely ineffective if the infringing content has spread so quickly and so far that it is unmanageable: even those who have successfully asserted their personality rights in court must assume that the illegal content will appear elsewhere.[129]

### 4.4.2 Cyberbullying and Cyberstalking

#### 4.4.2.1 Background

A specific form of infringement of personality rights is cyberbullying or cybermobbing[130], i.e. the sharing of defamatory text, images or films using modern means of communication (mobile phone, instant messenger services, social networks, video sharing sites, forums and blogs) to slander, ridicule or harass people[131]; the attacks are generally repeated or take place over a long period of time[132].

Cyberstalking is the use of electronic communication, e.g. social networks, in order to harass third parties. Stalking is defined as the repeated persecution or harassment of a person. This can take place in the form of monitoring, spying or contact. Stalking often takes place between people who

---

[125] Decision of the Swiss Federal Supreme Court 113 II 369 E. 3 p. 371.

[126] cf. for example Barrelet Denis/Werly Stéphane, Droit de la communication, Bern 2011, N 1683.

[127] See also Schneider-Marfels Karl-Jascha, Facebook, Twitter & Co: "Imperium in imperio", Jusletter, 20 February 2012.

[128] cf. the decision on a blog platform operated by the Tribune de Genève (FSC 5A_792/2011 of 14/01/2013).

[129] Ladeur Karl-Heinz/Gostomzyk Tobias, Der Schutz von Persönlichkeitsrechten gegen Meinungsäusserungen in Blogs, Neue Juristische Wochenschrift NJW 2012, p. 713.

[130] The two terms are used interchangeably in this report.

[131] A study conducted in the cantons of Valais, Thurgau and Ticino between November 2010 and June 2012 with 960 students – 49% female with a mean age of 13.5 years – indicated that the number of cyberbullying victims and offenders is very low; however, the study also indicates an increase in incidents between 2010 and 2012. See: Unpublished figures from the netTEEN-Studie (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, University of Zurich). Moreover, among adolescents cyberbullying often seems to be closely connected to traditional forms of bullying, as online victims and perpetrators are usually also involved offline. See: Perren Sonja, Professionswissen für Lehrerinnen und Lehrer – Grundlagen für die Aus- und Weiterbildung von Lehrerinnen und Lehrern, eds.: H.U. Grunder, K. Kansteiner-Schänzlin, H.Moser, p. 15.

[132] Bericht des Bundesrates vom 26.05.2010 "Schutz vor Cyberbullying" [Report of the Federal Council of 26.05.2010 on "Protection from Cyberbullying"]; available at: http://www.ejpd.admin.ch/ejpd/de/home/dokumentation/info/2010/ref_2010-06-02.html (only available in German, French and Italian).

already know each other or were previously close to each other. In addition to online harassment, the data provided on social networks by users themselves can also be used in order to identify potential victims' addresses, study their everyday habits and follow them physically.

The phenomena of cyberstalking and cyberbullying are not limited to social networks; however, they are increasingly taking place on these sites and are subject to special circumstances[133]. The ability to use social networks under a pseudonym allows offenders space for anonymous action, which facilitates the harassment or humiliation of others. Such acts of infringement can also be made on social networks in such a way that they are visible to third parties, which increases the impact on the victim.

#### 4.4.2.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for the exchange of "best practices" for the prevention of cyberbullying (and cybergrooming). Moreover, it calls for platform operators to make effective complaints mechanisms available and carefully monitor incoming complaints.

The "klicksafe" awareness campaign commissioned by the European Commission to promote media literacy and adequate handling of the internet and new media provides information on the internet including information on the phenomena of cyberbullying, outlines the existing law and gives general advice to those concerned on how to deal with the situation in an appropriate manner[134].

South Korea attempted to combat serious incidents of cyberbullying and concerns regarding fairness in relation to political elections[135] with an identity requirement on social networks[136]. The decision of South Korea's Constitutional Court on the unconstitutional nature of an identity requirement[137], countless hacker attacks on the servers of the providers of the affected sites and the theft of the personal data of millions of South Koreans led the Korean Communications Commission to decide to abolish the identity requirement system in 2014[138]. A licensing requirement for news websites with more than 50,000 users was introduced in Singapore in June 2013.[139]

#### 4.4.2.3 Legal status in Switzerland

Swiss law does not contain any specific cyberstalking or cyberbullying provision. Nevertheless, existing criminal and civil law cover many of the actions that can be assigned to the two terms if they are committed with the aid of electronic means of communication. The Federal Council's Report on cyber-

---

[133] In its 2011 Annual Report 2011, CYCO noted that complaints of threats and coercion had increased and that social networks were increasingly being used for this purpose. They also found that 30 of the reported cases of cyberbullying fell under the categories "threats, defamation and coercion"; however, no information was provided as to whether this occurred on social networks or via e-mail. (see CYCO Annual Report p. 6). According to a CYCO internal communication to the Annual Report 2011, nine of the reported defamation incidents were committed via/on social networks and three incidents in the category "Threatening behaviour, coercion and extortion" took place on social networks. However, this marked increase was not confirmed in 2012 and in the opinion of the CYCO therefore does not represent a discernible trend (CYCO Annual Report 2012, p 9).

[134] See http://www.klicksafe.de/ueber-klicksafe/die-initiative/project-information-en/.

[135] Introduction of a system for the compulsory identification of persons who express themselves for or against political candidates on websites or the internet forums in the Public Officials Election Act (POEA) in 2005.

[136] See Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mission to the Republic of Korea, 21.03.2011, A/HRC/17/27/Add.2 and a country profile for South Korea on the OpenNet Initiative, available at: http://www.access-controlled.net/profiles/.

[137] South Korea's Constitutional Court declared the requirement to disclosure identity as unconstitutional: "South Korea's real-name net law is rejected by court", 23.08.2012; available at: http://www.bbc.co.uk/news/technology-19357160.

[138] See Kate Jee-Hyung Kim, Lessons Learned from South Korea's Real-Name Policy, 17.01.2012, available at: http://www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-name-verification-system and "Real-name Internet law on way out", Korea Joonang Daily, 30.12.2011; available at: http://koreajoongangdaily.joinsmsn.com/news/article/article.aspx?aid=2946369.

[139] cf. Neue Zürcher Zeitung no. 123, 31.5.2013, p. 5: Lizenzpflicht für Onlinemedien – Singapur verschärft die Aufsicht über Nachrichtenportale im Internet.

bullying also notes that at present there is no indication of the limits of the existing criminal justice system[140].

In cases of behaviour that constitutes cyberstalking or cyberbullying, defamation under criminal law (Art. 173-178 SCC) and civil law (Art. 28f. CC) are applicable. In addition to the rights derived from Art. 28a CC affected persons can also assert protection from infringement of personality rights in the form of violence, threatening behaviour or stalking before a court; the code states that third parties are to be prohibited from making any contact – which explicitly includes electronic communication – with them (Art. 28b para. 1 no. 3 CC).

Further protection may be granted under Art. 135 (Representations of acts of violence), 143$^{bis}$ (Unauthorised access to a data processing system), 144$^{bis}$ (Damage to data), 156 (Extortion), 179$^{novies}$ (Obtaining personal data without authorisation), 180 (Threatening behaviour), 181 (Coercion), 197 (Pornography) and 198 (Sexual harassment) of the Swiss Criminal Code.

Again, the most significant difficulties are in the field of law enforcement; however, determining the identity of the offender should be simplified by the fact that the offender often shares the same social environment as the person concerned (school, work, etc.). In 2012, CYCO determined a decline in reports of criminal acts of defamation. One reason for this could be greater awareness about the use of social media due to the increased media coverage of cases of cyberbullying. [141]

### 4.4.3 Identity theft and other threats of malicious manipulation

#### 4.4.3.1 Background

*Identity theft* is simple on many social networks. In the field of internet crime, identity theft and fraud are increasing on social networks; these often serve the perpetration of pecuniary offences[142]. Moreover, identity theft can serve to damage the reputation of third parties or otherwise infringe the personality rights or honour of third parties. Users create a profile with the name of a famous person and take advantage of their celebrity or damage their reputation by malicious behaviour. Similarly, it is possible to open profiles in the name of a person from one's personal environment in order to harm this person by making them the subject of ridicule or sending illegal or harmful content in their name.

The creation of a *fantasy identity* on social networks can provide users with advantages that they would not be granted if they were to reveal their true identity. By doing so they can infiltrate social circles to which they otherwise would not have access or establish close online friendships with people who would treat them differently if they were aware of their true identity.

Stolen or fictitious identities can be used for various malicious purposes, such as for collecting information for illegal purposes, grooming, cyberstalking, cyberbullying, phishing, spamming, or spreading computer viruses.

#### 4.4.3.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for the establishment of adequate complaint mechanisms against malicious behaviour on social networks with a particular

---

[140] Bericht des Bundesrates vom 26.05.2010 "Schutz vor Cyberbullying" [Report of the Federal Council of 26.05.2010 on "Protection from Cyberbullying"]. The Federal Council also rejected the introduction of new elements of a crime for bullying at work (as requested in the Freysinger Motion 10.4054), because current law already largely regulates the behaviour in question and the introduction of another penal provision would provide no additional benefit in view of the fact that this would also not counter the central problems of demonstrability and of the repression of the person concerned. See http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20104054 (only available in German, French and Italian). The National Council also rejected the introduction of bullying as an element of a crime with 130 to 33 votes and 11 abstentions.

[141] CYCO Annual Report 2012, p. 9.

[142] ENISA Threat Landscape Report of 28.09.2012, p. 21ff.; available at: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape.

focus on identity theft. It also recommends that member states commit platform operators to using the most effective security measures to protect personal data from unlawful access by third parties. This should include the encryption of communication between users and the website of the platform operator. Moreover, it recommends that platform operators inform users of breaches of security measures so that they can take preventive measures, such as changing their password.

The European Commission proposes the establishment of an EU Centre to combat cybercrime[143]; this is to be dedicated to issues such as the protection of user profiles on social networks from digital abuse in order to take measures against identity theft on the internet[144].

#### 4.4.3.3 Legal status in Switzerland

If a third party creates a user profile on a social network using a protected name and without the consent of the beneficiaries, they typically violate the protection of one's name under civil law in accordance with Art. 29 para. 2 CC. The regulation protects the person concerned against unauthorised appropriation of their name by third parties. It covers the civil and official names of natural persons, but also pseudonyms, nicknames, abbreviations, acronyms and abbreviated names insofar as these are perceived by the public as the name of the namebearer[145].

It is likely that there will be an infringement of the individual's right to their own image in accordance with Art. 28 CC if an unauthorised person uses images of another person in order to establish a user profile with their identity.

On social networks that also provide private communication (e.g. Facebook), a possible violation of confidentiality or privacy in accordance with Art. 28 CC exists if a third party infiltrates other user profiles and is thus party to private communication that was not made available to them by the data subject. The use of third-party names and user profiles established in a third-party name for the purpose of causing others to divulge private information using a fraudulent identity is also prohibited.

From the perspective of data protection, the acquisition of personal data using a false identity may be a violation of the principle of visibility of data collection and the principle of good faith (Art. 4 para. 2 and 4 FADP)[146]. If a third party publishes sensitive personal data regarding the data subject on a user profile that has been established in a third-party name, this action constitutes a violation of Art. 12 para. 2 lit. c FADP.

If third parties hack into other user profiles without authorisation, become party to information that is not freely accessible, change content or the login passwords of the authorised user, this may constitute an offence of unauthorised access to a data processing system (Article 143$^{bis}$ SCC), damage to data (Art. 144$^{bis}$ SCC) and/or obtaining personal data without authorisation (Art. 179$^{novies}$ SCC).

User profiles established using a false identity and fantasy profiles can serve a wide variety of unlawful purposes. These are primarily pecuniary offences, defamation, coercion and threatening behaviour (Art. 173-177, 146, 147, 156, 180, 181 SCC) infringement of personality rights and stalking (Art. 28 para. 1 no. 28b. 3 CC). Art. 3 para. 1. lit. o UCA, offers protection from spamming, while Art. 144$^{bis}$ SCC (damage to data) covers both the operation and distribution of viruses by means of social networks.

---

143 Communication on Tackling Crime in the Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final.

144 EU Commission Press Release of 28.03.2012 "An EU Cybercrime Centre to fight online criminals and protect e-Consumers", IP/12/317.

145 BSK-DSG, Bühler Roland, 4$^{th}$ ed., Basel 2010, Art. 29, p. 321f. margin number 4, 7, p. 325 margin number 16.

146 Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 81 no. 14, p. 99 no. 56.

Effective action can be taken against phishing and dissemination of malware on .ch domains pursuant to Art. 14$^{bis}$ of the Ordinance of 6 October 1997 on Addressing Resources in the Telecommunications Sector.[147] In individual cases this may also be useful against the use of false identities.

The analysis demonstrates that the substantive law largely covers the offences associated with digital identity fraud. Nevertheless, in reality it may prove difficult to determine the perpetrator's identity in order to proceed against them, especially in the case of professional criminals.

### 4.4.4 Monitoring of statements made on social media (social media monitoring)

#### 4.4.4.1 Background

Companies, government agencies, organisations and certain private individuals have an interest in information regarding the issue of what is reported about them in social media. Through systematic and continuous monitoring, interested organisations may attempt to (re-)gain control of their representation. Automated tools are used in order to cope with the unstructured flow of information.

A problem of social media monitoring is that it acquires not only the content of information shared on networks, but also information about their authors. Persons conducting monitoring obtain information about the real names or at least the pseudonyms of authors and sometimes information regarding age, gender, occupation, employer, area of origin, and any other information disclosed. Information on world views and political attitudes is particularly sensitive.

#### 4.4.4.2 Legal status in Switzerland

Not all options to process data in networks that are technically possible are automatically covered by the principle of purpose limitation. According to the Data Protection Act, even published data may not simply be used for other purposes. Personal information on social media platforms is often addressed only to personal friends or it is published only in a particular environment or a particular context. Without transparent information on social media monitoring, data subjects lack at the very least the required knowledge on the use of personal data for monitoring. Members of social media platforms must at the very least be aware from the circumstances that monitoring tools are being used. If personal data is published about third parties, the knowledge and consent of these third parties will in any event be lacking. For these reasons it cannot be assumed in many cases that the persons concerned have made the personal information generally available on social media platforms within the meaning of Art. 12 para. 3 FADP.

On its website, the FDPIC has issued recommendations for privacy-compliant implementation of social media monitoring. [148] The aim is to keep the processing of personal data to the minimum necessary for the purpose of evaluation and to delete them or make them anonymous as soon as possible. It does not seek to include private personal information (especially from closed user groups or circles of friends) and recommends that monitoring should be limited to the analysis of public opinions and comments.

---

147 SR 784.104

148 http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00692/ (only available in German, French and Italian)

## 4.5 Impairment of common interests

### 4.5.1 Racist and other discriminatory statements ("hate speech")

#### 4.5.1.1 Background

As with the internet in general, social networks also provide a platform for easy dissemination of racist content using images, text and videos[149]. In addition, platforms can be used to organise racist associations and to recruit new members.

Social networks can also be misused to discriminate against people on the basis of characteristics other than race, e.g. sexual orientation, origin, religion, disability, lifestyle, language, social status, political or ideological conviction, gender or age.

Control and deletion of racist and discriminatory material is made more difficult on social networks than on websites, because the distribution of content and networking of people in these forums is even easier and faster than is possible via websites.

In proceedings against discriminatory statements on social networks the problem may also arise that the legal status in relation to racist and otherwise discriminatory content differs from one country to another. Consequently, content that is illegal in Switzerland may be legal abroad[150]. In the case of internationally accessible media this leads to difficulties in dealing with such content; a general tendency can be observed towards operators of social networking sites blocking upon request certain types of content in those countries where they are punishable. For example, Twitter blocked the user account of a right-wing extremist organisation that had been banned in Germany for those Twitter users who specify Germany as their country in their account settings[151].

#### 4.5.1.2 Solutions in other countries and in international law

The Additional Protocol to the Convention on Cybercrime of the Council of Europe concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems of 28 January 2003 explicitly focuses on the dissemination of racist and xenophobic content on the internet, among other things. The Convention of the Council of Europe of 23 November 2001[152] on Cybercrime (CCC) entered into force in Switzerland on 1 January 2012. Although the Additional Protocol was approved by the Federal Council, it has not yet entered into force in Switzerland.

The site jugendschutz.net was founded[153] on the basis of § 18 of the Jugendmedienschutz-Staatsvertrag - JMStV (Interstate Treaty on the Protection of Minors)[154] between the German federal states. In Germany, jugendschutz.net is active in combating racist and discriminatory content on the internet and social networks. Moreover, the organisation raises public awareness by way of prevention days, training programmes and publications, such as the brochure "Klickt's? Geh Nazis nicht ins Netz!" [Has it clicked? No Nazis on the Internet][155]. Consequently, their work is particularly directed

---

[149] According to a CYCO internal communication to the Annual Report 2011, social networks were the instrument/site of nine of the approx.. 30 reported incidents of racial discrimination in 2011.

[150] "Hate speech" enjoys much more extensive protection in the USA than in most Western European countries. See the decision of the French Tribunal de Grande Instance de Paris, LICRA vs. Yahoo! of 22.05.2000, in which the French court declared the sale of Nazi memorabilia - which is permitted under US law, but not under French criminal law - on Yahoo's auction site illegal.

[151] "Erste landesspezifische Sperre auf Twitter: Account von verbotener rechtsextremistischer Vereinigung in Deutschland gesperrt"; available at: https://netzpolitik.org/2012/erste-landesspezifische-sperre-auf-twitter-account-von-verbotener-rechtsextremistischer-vereinigung-in-deutschland-gesperrt/ (only available in German).

[152] SR 0.311.43.

[153] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien, Bay.GVBI no. 5/2003, p 147ff. [Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia of 10 - 27 September 2002, Bay.GVBI no. 5/2003].

[154] http://www.jugendschutz.net/ (only available in German).

[155] http://www.jugendschutz.net/materialien/klickts.html (only available in German).

against the extensive use of social networks by right-wing extremists. Another example of a German platform with a similar orientation is Netz-Gegen-Nazis.de[156].

The INACH (International Network Against Cyberhate)[157] initiative, which was founded by jugendschutz.net, is internationally active against the dissemination of and incitement to hatred on the internet, with a particular focus on bullying on social networks. The network is made up of hotlines for different states; these exchange best-practice strategies and work towards the deletion of discriminatory and illegal content and websites on the internet.

#### 4.5.1.3 Legal status in Switzerland

Art. 261$^{bis}$ SCC prohibits various forms of discrimination against persons by private individuals on the basis of their race, ethnicity or religion. This provision essentially covers all conceivable forms of communication in social networks, whether in the form of photos, videos, pictures or text. The precondition, however, is that communication is *open*[158]. In jurisprudence[159], statements on social networks are regarded as in the public domain if the target audience is not limited to persons who are connected by a relationship of trust (e.g. by restrictive privacy settings on Facebook).

In Swiss court practice there have already been various convictions for racist remarks on social networks.[160] Art. 261$^{bis}$ SCC, however, only covers discrimination based on race, ethnicity and religion and therefore not all of the characteristics listed in the constitutional prohibition of discrimination (Art. 8 para. 2 of the Federal Constitution) such as gender, age, disability or sexual orientation. Only personality rights (Article 28f. CC) offer a certain level of protection if a person is discriminated against on a social network on the basis of characteristics related to their personality.

At the federal level, the Federal Commission against Racism (FCR)[161] and the Cybercrime Coordination Unit Switzerland (CYCO)[162] combat racism on the internet. If the FCR is made aware of racism on social networks, it reports this to CYCO, which, after an initial inspection and data archiving, forwards this[163] to the relevant domestic and international law enforcement agencies. CYCO is also an independent body that searches the internet for criminal content and creates detailed analyses of cybercrime. Since the operators of many social networks are based abroad, prosecution is often difficult, especially when it comes to revealing the identity of an unknown author. According to CYCO, the deletion of allegedly illegal content does not generally pose a problem in practice. The dissemination of racist or otherwise discriminatory content is prohibited in the conditions of use of many social networks, and if such content is reported, operators authorise its deletion as a matter of principle.

### 4.5.2 Pornography

#### 4.5.2.1 Background

As in other areas of the internet, problems with the distribution of pornography via social networks may arise if these qualify as hard-core pornography (i.e. portrayals of sexual acts with children [paedopornography] or animals in accordance with Art. 197 para. 3 SCC) or soft-core pornography that is ac-

---

156 http://www.netz-gegen-nazis.de/ (only available in German).

157 http://www.inach.net.

158 For a broad interpretation of the notion of the public domain by the Federal Court see Decision of the Federal Supreme Court 130 IV 111.

159 cf. Fiolka Gerhard, Basler Kommentar Strafrecht II, 3rd ed. Basel 2013, before Art. 258 no. 25.

160 An example of this is a Facebook comment made against a dark-skinned classmate (Entscheid Nr. 2010-32 in der Sammlung Rechtsfälle der Eidg. Kommission gegen Rassismus [Decision no. 2010-32 in the collection of legal cases of the Federal Commission against Racism; http://www.ekr.admin.ch/dienstleistungen/00169/ - only available in German and French).

161 http://www.ekr.admin.ch/aktuell/index.html (only available in German and French).

162 http://www.cybercrime.admin.ch/kobik/de/home.html .

163 In 2012, reports of racial discrimination only accounted for 0.78 % of all reports received, CYCO Annual Report 2012, p. 4.

cessible by persons under 16 years of age. For the purposes of this report, the main focus will be on the issue of child pornography (paedopornography).

As child pornography is strictly prohibited worldwide, rings of offenders normally use distribution and communication channels that operate with greater anonymity and secrecy than traditional social networks. Representations of the sexual abuse of children are sold via commercial websites or exchanged in closed user groups or peer-to-peer networks[164]. The latter allows the discrete and anonymous exchange of child pornography[165]. The publication or distribution of child pornography on open platforms is in practice therefore very rare.

#### 4.5.2.2 Solutions in other countries and in international law

The Convention of the Council of Europe of 23 November 2001 on Cybercrime (SR 0.311.43), which is also binding for Switzerland, serves to improve cooperation between member states, which is particularly important in view of the frequent cross-border nature of internet issues. Art. 9 of the Convention contains a relatively comprehensive provision on criminal liability for acts related to child pornography.

Various organisations in different countries are dedicated to locating and deleting harmful and illegal content on the internet. In England, for example, there is the Internet Watch Foundation, whose tasks include investigating child pornography on the internet[166].

It is expected that as a result of Switzerland's accession to the Convention of the Council of Europe on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25.10.2007 the intentional consumption of hard-core pornography – which includes simply viewing such content on social networks without downloading it – will in the future be illegal[167].

#### 4.5.2.3 Legal status in Switzerland

Art. 197 SCC protects people under 16 years against any, and adults against any unsolicited, confrontation with pornography. Moreover, the provision prohibits hard-core pornography. Art. 197 SCC covers most actions and objects of offence that could lead to soft-core pornography reaching the wrong recipient via social networks or hard-core pornography being distributed via social networks. If pornographic content is published without effective access restriction on social networks – e.g. in the form of a YouTube video – this means that it becomes accessible to persons under 16. A warning on a website that disappears by clicking on it is, for example, insufficient[168], as is the restriction of use of a website using a password if there is a lack of age verification[169].

Pornography – including soft-core pornography – is among the content usually prohibited by most platform operators in their conditions of use and in the event that it does appear can be quickly and simply deleted thanks to relatively rigid "notice-and-take-down" functions and filtering software.

The often international context in the case of the distribution of illegal pornography constitutes a major challenge to law enforcement authorities, particularly due to differences in regulations and measures

---

[164] Information from the Cybercrime Coordination Unit Switzerland on the subject of child pornography, http://www.cybercrime.admin.ch/content/kobik/en/home/themen/kinderpornografie.html.

[165] See press release by the Federal Office of Police "Trotz Rückgang der Verdachtsmeldungen: Kinderpornografie bleibt die meistgemeldete Kategorie bei KOBIK", 03.04.2012, http://www.fedpol.admin.ch/content/fedpol/de/home/dokumentation/medieninformationen/2012/2012-04-03.html (only available in German, French and Italian).

[166] http://www.iwf.org.uk/.

[167] BBl 2012 7618 and BBl 2012 7657.

[168] Decision of the Swiss Federal Supreme Court 131 IV 64 E. 10.3.

[169] Decision of the Federal Supreme Court 6S.26/2005 E. 3.2.

between the various legal systems. The number of reports CYCO receives regarding illegal pornography (especially involving children) is consistently high. [170] Furthermore, CYCO is also involved on a federal level in the investigation of child pornography; this involvement includes research without reason for suspicion.

### 4.5.3 Threats to public order by mass mobilisation

#### 4.5.3.1 Background

Social platforms are potentially valuable for a democratic society in that they can make a significant contribution to the formation of opinion and to political expression, especially for minorities. In certain constellations they are capable of mobilising large numbers of people in a short period of time.[171] However, in extreme cases this can have negative consequences and a significant negative impact on public order.

For example, there was a call to attend a mass gathering called "Tanz dich frei" [Dance yourself free] via Facebook at which a violent minority caused considerable damage to the city centre of Bern in May 2013. As a private claimant in the criminal proceedings, the city filed petitions including one against Facebook stating that it had to release the identification data of the relevant Facebook account. [172]

#### 4.5.3.2 Solutions in other countries and in international law

The problems of mobilisation via social networks can be illustrated by the example of serious disturbances in the small Dutch town of Haren on 21 September 2012. The trigger was a Facebook entry made by a young girl who forgot to mark an invitation to her 16th birthday as a private party. A call for a "Project X Party", which was followed by several thousand young persons, was disseminated at incredible speed via Twitter and Facebook. The originally peaceful mood turned – not least due to the influence of alcohol – into large-scale aggression, which the law enforcement officers present were unable to cope with due to various failures.

In a report published in March 2013 an investigation commission recommended that authorities acquire knowledge of how social media operates. Thanks to targeted monitoring of the platforms they should in future be able to detect such threats to public order in good time – without the need for systematic monitoring of individuals – and steer them in a safe direction. The report recommends that authorities should urge operators of social platforms to remove any call to unlawful activities. Furthermore, it recommends that operators highlight, particularly to their younger customers, the risks entailed by the typical social media mix of private and public communication.[173]

#### 4.5.3.3 Legal status in Switzerland

If a call prompts in any person the intent to commit a specific offence (e.g. damage to property) punishment for incitement to this offence may be considered (Art. 24 SCC). In this case the instigating party is subject to the same penalty as the offender. Furthermore, according to the Swiss Criminal Code, public incitement to commit a felony or act of violence (Art. 259 SCC) is punishable with a custodial sentence of up to three years or a fine. The call does not have to refer to well-defined actions, nor does it have to be addressed to specific individuals. However, according to Swiss courts it must

---

[170] In 2012 the percentage of reports of suspicions of prohibited child pornography accounted for approximately a third of the total number of reports received; CYCO Annual Report 2012, p. 4.

[171] cf. Section 3.2 as regards the opportunities offered by social media for diverse and lively communication.

[172] Press release by the City of Bern, 12 June 2013: http://www.bern.ch/mediencenter/aktuell_ptk_sta/2013/06/strafanzeige/view?searchterm=tanz dich frei (only available in German).

[173] Report of the Commission on "Project X – Haren" of 08.03.2013, p. 31ff.; available at http://de.scribd.com/doc/129273298/Hoofdrapport-rellen-Haren (only available in Dutch).

demonstrate a certain urgency, although a clear call may also exist if a person appropriates third-party messages (retweeting)[174].

On the other hand, the penal provision does not cover the mere call to participate in an unauthorised event. However, this may violate cantonal or municipal regulations[175]. As with other penal provisions (e.g., the penal provision on racial discrimination, cf. Section 4.5.1.3), in Art. 259 SCC the question arises as to whether a statement on a social platform should be classified as public or as private.

Like defamation, incitement in accordance with Art. 259 can also fall under the special rules for criminal liability of the media (Art. 28 SCC)[176]. According to this regulation, the author of the public invitation has sole legal responsibility. The only alternative is the responsible editor or the person responsible for publication if the author cannot be determined or cannot be prosecuted in Switzerland.

In relation to the prosecution of authors of illegal content on platforms cf. Section 5.2 and in relation to blocking and deletion measures cf. Section5.4.

### 4.5.4 Threats to public health

#### 4.5.4.1 Background

Social networks are used to share information on a wide range of interests. Depending on subject and motivation this can also have negative impacts on users' health or social status. For example, online forums on which people interested in suicide, eating disorders and self-harm communicate with each other may even glorify or inspire and encourage such acts and phenomena. This can lead to a trivialisation of the problem, reinforce existing self-destructive tendencies, and in the worst case promote the execution of specific harmful actions. However, in addition to these risks, the internet also offers supportive information on such problems to those concerned[177].

Another problem is posed by the numerous online forums that exchange information on diseases, drugs and treatments whose quality is not verifiable or very difficult to verify. 44% of the Swiss population obtains information about health issues via the internet; the internet is mainly used for complementary information in addition to an exchange with experts or trusted lay persons. It is assumed that the demand for both health information on the internet and participative web applications will increase. Two out of three people who inform themselves about health issues using the internet do not trust the information found there[178]. The establishment of controls or certificates in the online health sector increases the confidence of this part of the population. For less suspicious users, the risk remains that they may obtain subjective or false information on online portals in relation to health issues, which in the worst case could have negative consequences for their health.

#### 4.5.4.2 Solutions in other countries and in international law

The site jugendschutz.net, which was established by the German federal states, also provides information on the risks and hazards associated with portals that glorify or promote suicide, eating disorders and self-harm and are thus dangerous for young people[179]. Jugendschutz.net informs those con-

---

[174] Fiolka Gerhard, Basler Kommentar Strafrecht II, 3rd ed. Basel 2013, Art. 259 no. 12.

[175] cf. Art. 8 des Reglements der Stadt Bern über Kundgebungen auf öffentlichem Grund [Art. 8 of the Regulations of the City of Bern on demonstrations on public land] http://www.bern.ch/leben_in_bern/stadt/recht/dateien/143.1/ (only available in German).

[176] cf. Zeller Franz, Gerhard, Basler Kommentar Strafrecht II, 3rd ed. Basel 2013, Art. 28 no. 65.

[177] See, for example, the Arbeitsgemeinschaft Ess-Störungen - AES [Working Group on Eating Disorders], available at: www.aes.ch (only available in German).

[178] For more information on this subject see: eHealth Suisse Bericht Öffentliches Gesundheitsportal [eHealth Suisse Report Public Health Portal], adopted by the Steering Committee on 26.01.2012 p. 6, 7, 11 (only available in German, French and Italian).

[179] http://www.jugendschutz.net/selbstgefaehrdung (only available in German).

cerned and parents, reviews relevant internet sites and works towards removing problematic content. It also raises the awareness of operators of social networks regarding the subject and offers providers that wish to delete such content a replacement website on the subject of eating disorders that links to educational initiatives and counselling[180].

Based on § 18 para. 1 of the German Protection of Young Persons Act[181], the responsible review board[182] can place media and telemedia that are likely to endanger the development of children or young people on a blacklist of media harmful for young people. The BPjM's blacklist includes forums that glorify eating disorders or suicide[183].

#### 4.5.4.3 Legal status in Switzerland

Communication between like-minded private individuals on topics such as suicide fantasies, eating disorders, self-harm, etc., fundamentally falls within the scope of freedom of expression. There is no legal basis that would specifically cover the phenomenon if it were to have an obviously damaging effect on society. In principle, the Confederation can assume an informative role to protect the health of the population. The Federal Office of Public Health (FOPH) is active in many areas that are connected to the subjects of suicide, eating disorders and self-harm. However, to date the FOPH has not explicitly dealt with actions via social media that could have promoted actions harmful to health.

There is currently no legal basis that would restrict communication about drugs and treatment methods between private individuals, as long as they are not active in an advertising capacity[184]. According to the FOPH, greater transparency is essential in relation to health information and health forums on the internet. However, to date, quality labels for reliable health information on the internet[185] have related primarily to websites rather than social media.

### 4.5.5 Manipulation of the formation of opinion for commercial reasons

#### 4.5.5.1 Background

Social networks can be used by companies to distribute via paid actors, who pose as independent consumers, positive or misleading information about their goods or services. Only a small number of people is necessary to simulate the activities of a large group. This can also occur using "flogs" (fake blogs) or "sockpuppets" (false online identities), which appear independent, but are used exclusively for advertising purposes. The methods described can also be used to negatively portray competing companies and their products and services.

Other problems may arise from the communication format of a social network. If Twitter, for example, is used for promotional purposes, text is limited to 140 characters, which means that transparency regarding the author, background, cause and motivation of individual messages may fall victim to space restrictions.

---

[180] http://www.anaundmia.de/ (only available in German).

[181] Jugendschutzgesetz vom 23.07.2002, BGBl. I S. 2730 [Protection of Young Persons Act of 23.07.2002, Federal Law Gazette I].

[182] http://www.bundespruefstelle.de/ (only available in German).

[183] See for example the BPjM's decision on blacklisting an anorexia blog: BPjM-Entscheid Nr. 5601 vom 04.12.2008 – "Pro Ana" [Decision of the Federal Review Board for Media Harmful to Minors no. 5601 of 04.12.2008]; available at: http://www.doerre.com/jugendschutz/20081204_bpjm_index.pdf (only available in German).

[184] Art 31f. of the Federal Act of 15 December 2000 on Medicinal Products and Medical Devices (TPA), CC 812.21 and the Ordinance of 17 October 2001 on the Advertising of Therapeutic Products (TPAO), CC 812.212.5, which in Art. 4 lit. c includes as professional advertising of therapeutic products advertising that uses audiovisual means and other image, sound and data media as well as data transmission systems such as the internet.

[185] One example is the quality label, the Health on the Net Foundation (HON), www.hon.ch.

#### 4.5.5.2 Solutions in other countries and in international law

Within the EU there has been a response to the phenomenon of non-transparent methods of advertising on social networks[186]. The EU Directive on Consumer Rights[187], which governs the conclusion of contracts between businesses and consumers, is concerned with the fulfilment of the company's duty to provide information in view of technical constraints such as the limited number of characters on small displays. The Directive formulates the minimum requirements for the duty to provide information and calls for consumers to be made aware of other sources of information, e.g. in the form of free-of-charge numbers or hypertext links to the company's website. This regulation is interesting in the context of social networks, because certain services, such as Twitter, are characterised by a limited number of characters. Moreover, increasing numbers of users are logging on to social networks via mobile means of communication, which gives rise to information and space problems due to the terminal (e.g. smartphone) used.

The US agency for consumer protection and competition law, the Federal Trade Commission (FTC), has issued guidelines on consumer protection from unfair and deceptive advertising[188] to help advertisers comply with the law[189]. The guidelines call for financial and material connections (payments or gifts) between advertisers and third parties advertising on their behalf (including bloggers, celebrities, etc.) to be disclosed when campaigning on social networks (including social networks with a limited number of characters such as Twitter)[190].

#### 4.5.5.3 Legal status in Switzerland

The provisions of the Federal Act against Unfair Competition[191], which regulate advertising activity independently of specific products, industries or media, are also applicable to the internet and therefore also to competition-related activities on social networks[192].

The general provisions of Art. 2 UCA include as unfair behaviour advertorials as well as misrepresentative and misleading advertising with regard to the promotional nature of advertising[193]. If private individuals receive free products or payments in return for positive statements about a company and its products and services on their blogs or networking profiles and this fact is not made transparent, this behaviour may be unfair within the meaning of the general provision of Art. 2 UCA[194], insofar as the behaviour is objectively likely to influence the efficiency of the market concerned. Misleading advertising may be further covered by Art. 3 para. 1 lit. b and i UCA. The recent revision of the UCA intro-

---

[186] In its resolution on the impact of advertising on consumer behaviour (2010/2052 (INI)) (17), the EU Parliament criticises new forms of surreptitious advertising on the internet that are not covered by the Unfair Commercial Practices Directive. In doing so it refers directly to commercial statements and advertising messages by companies on blogs, social networks or similar forums that give the appearance of being the opinions of independent consumers. The is encouraging member states to introduce observers in order to monitor potentially surreptitious advertising on such forums.

[187] Directive 2011/83/EU on consumer rights, amending Directive 93/13/EEC and Directive 1999/44/EC repealing Directive 85/577/EEC and Directive 97/7/EC.

[188] Guides Concerning the Use of Endorsements and Testimonials in Advertising, FTC 16 CFR Part 255; available at: http://www.ftc.gov/os/2009/10/091005revisedendorsementguides.pdf.

[189] In particular, Section 5 Federal Trade Commission Act (15 U.S.C. 45) in relation to the use of endorsements and testimonials in advertising; available at: http://www.ftc.gov/ogc/ftcact.shtm . The FTC monitors compliance with the guidelines; in the event of a breach thereof, the commission may carry out an investigation into whether the affected practice is violating the law, see: http://www.ftc.gov/opa/2009/10/endortest.shtm.

[190] The guidelines also recommend advertisers to comprehensively explain to bloggers, celebrities and other persons engaged in advertising activities on the advertiser's behalf the characteristics of the product and the legal status in order to prevent misleading advertising claims. In addition, the guidelines recommend reviewing the accuracy and appropriateness of advertising claims made by third parties engaged by advertisers. Advertisers and persons engaged in advertising activities on the advertiser's behalf are liable for false or misleading statements about the product.

[191] Federal Act of 19 December 1986 on Unfair Competition (UCA), CC 241.

[192] Jöhri Yvonne, Werbung im Internet, Zurich 2000, p. 59.

[193] Jung Peter/Spitz Philippe (eds.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, p. 180f.; Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zurich 2011, p. 52.

[194] Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zurich 2011, p. 71f.

duced Art. 3 para. 1 lit. s UCA[195], which provides for binding disclosure requirements to increase transparency in electronic commerce.

If paid or otherwise compensated private third parties are instructed by companies to use their social network presence in order to negatively portray the company's competitors, Art. 3 para. 1 lit. a UCA may be applicable, insofar as the behaviour disparages the competition, its goods, works, services, prices or business relationships by means of incorrect, misleading or unnecessarily damaging statements[196].The difficulty in this area is particularly likely to lie in the recognition of the promotional nature of the social network presences of private individuals as well as in proving the connection between any private individual involved and a particular company.

### 4.5.6 Manipulation of the formation of public (political) opinion

#### 4.5.6.1 Background

Similar methods to the commercial sector can also be used in the formation of public opinion in order to influence political discourse, which in the run-up to elections and referendums seems particularly problematic. Profiles on social networks, networking groups and blogs are used to promote a candidate or specific policies under the semblance of independence. This phenomenon is known as "astroturfing".

Furthermore, there are software programs in development that allow individuals to manage multiple user accounts on blogs, internet forums and social networks, so as to create fake majority opinions[197].

#### 4.5.6.2 Legal status in Switzerland

The freedom of choice and freedom to vote according to Art. 34 para. 2 of the Federal Constitution also protects to a limited extent against the influence of private operators on the freedom of the citizen to form an opinion. Especially in the run-up to an election, the government has certain protective obligations. If shortly before election day private individuals publish content that is obviously false or misleading, the authorities must educate voters regarding the actions of the private individual or rectify the content. Rerunning the vote is possible in cases where it appears likely that the behaviour of private individuals has influenced the vote decisively and the authorities have not fulfilled their obligation to educate.

Consequently, the government should intervene in cases of clandestine political advertising on social networks when the concealment of the actual background of the social media presence could lead to misleading voters just before election day. The results of the vote will only be annulled if it appears probable that they have been decisively influenced by such non-transparent methods. If such an influence is undetectable and the behaviour in question does not take place in the period immediately prior to elections or voting, public discourse should rectify false or misleading statements made by private individuals[198].

---

[195] BBl 2011 4910.

[196] Jung Peter/Spitz Philippe (eds.), Bundesgesetz gegen den unlauteren Wettbewerb, Bern 2010, p. 226ff.

[197] "Security-Firma entwirft Tools zur Meinungsmache mit Kunstfiguren", heise online, 20.02.2011; available at: http://www.heise.de/newsticker/meldung/Security-Firma-entwirft-Tools-zur-Meinungsmache-mit-Kunstfiguren-1193436.html (only available in German).

[198] For information on this section see: Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, 4th ed., Bern 2008, p. 618f. and Häfelin Ulrich/Haller Walter/Keller Helen, Schweizerisches Bundesstaatsrecht, 8th ed., Zurich 2012, p. 443f. margin number. 1392ff.

### 4.5.7 Illegal advertising of certain products and services

#### 4.5.7.1 Background

In order to protect certain public interests, there are various prohibitions on advertising in Switzerland; it is possible for these to be ignored in communication on social networks. They concern, for example, the advertising of tobacco or certain medicines.

Compliance with regulations in the Federal Act on Alcohol (SR 680; Alcohol Act (AlcA)) are, for example, in the balance. The body responsible for compliance with the Alcohol Act, the Koordinationsstelle für Handel und Werbung - KHW [Co-ordination Office for Trade and Advertising][199] is often required to make decisions regarding Facebook presences. The problem it faces is that the non-product-related posts often do not originate from the page administrator, but are posted by users ("friends") voluntarily at the request of the page administrator.

#### 4.5.7.2 Legal status in Switzerland

Social media advertising campaigns that focus on Switzerland must in particular respect the advertising restrictions under Art. 42b AlcA. It also contains provisions on the protection of young persons. Art. 42b para. 3 lit e AlcA, for example, prohibits the advertising of distilled spirits "at events where the participants are primarily children and young people, or which are primarily intended for such persons". Whether such events can take place on social networks has not yet been determined.

In practice, the Swiss Alcohol Board ensures compliance with advertising regulations not only by means of administrative criminal law, but also by administrative law decisions. Statements made on social media raise various questions regarding enforcement of these regulations: Who is responsible for entries on a platform? How can a commercial provider of a social media presence that is based abroad be covered by law?

## 4.6 Special protection needs

### 4.6.1 Children and young people

#### 4.6.1.1 Background

The risks that may arise for children and young people on social networks are different in nature and go beyond the general impairments of individual interests that affect most users (as described above). Adult content, content that is harmful to young people or contact by third parties, especially those of a sexually motivated nature are particularly problematic[200]. Not all children and young people have the necessary technical skills and awareness to protect themselves from risks associated with problematic contact or the disclosure of personal data[201]. Furthermore, responsible persons, e.g. parents or teachers, often lack the necessary experience and expertise to provide children and young people with rational information on the risks of social networks. Friendships between students and teachers on social networks may represent another problem, as they carry the risk of inappropriate proximity. Moreover, such network contacts provide insights into the private lives of students and teachers that can put a strain on the relationship during teaching hours.

---

[199] The KHW only monitors advertising campaigns that have a clear connection to Switzerland (e.g. due to language, currency or distribution of the product).

[200] According to a recent study, sexual abuse via electronic media is widespread amongst young people in Switzerland. 9.5% of boys and 28% of girls claim to have been affected by this. "Cyber-victimisation" is therefore also an important sub-category of sexual abuse without physical contact. However, the information covers electronic media in general, which includes not only social networks, but also communication via mobile phone, e-mail, etc. See Optimus study "Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz", February 2012, p. 9, 29f., 96f. (Only available in German)

[201] According to the EU Kids Online 2011 study, which is based on data collected in 25 European countries, around 64% of children and young people aged between 11 and 16 know how to block unwanted messages by third parties and 56% know how to change their privacy settings on social networks. These numbers point to a large minority of children and young people who lack the necessary expertise to instigate the relevant protection measures. Moreover, 29% of 9-12 year-olds and 27% of 13-16 year-olds have their profiles set to public and a fifth of them provide information such as addresses and phone numbers on public profiles. See EU Kids Online Final Report, September 2011, p. 17.

One problem of technical feasibility for effective child protection on social networks is the inadequacy of the age verification systems that have been developed to date. These systems cannot ensure that the information provided by registrants matches their actual age[202].

#### 4.6.1.2 Solutions in other countries and in international law

The Council of Europe Recommendation on social networking services calls for the special protection of children and young people in the use of social networks. Furthermore, it recommends that providers make available preventive protection measures, establish reporting systems for problematic content and take action against cyberbullying and cybergrooming.

In addition, the Council of Europe calls on member states to examine ways of eliminating or deleting content created by children on the internet that could damage their dignity, security or privacy[203] and to expand their media skills[204]. In addition it also recommends the creation of protected space for children on the internet which should lead in particular to the introduction of a pan-European label for responsible certification systems for online content.[205]

The Proposal for an EU General Data Protection Regulation[206] also contains specific provisions for the protection of children. It recommends that the personal data of children *below the age of 13*[207] may be processed by information society services only with the parents' or guardian's consent. According to Art. 11, any information relating to data processing addressed specifically to children is to be provided in a form and language appropriate to the data subject's age.

The Safer Internet 2009-2013 programme[208] calls for the EU to raise public awareness, the establishment of a network of public contact points to report illegal and harmful content (grooming, cyberbullying, etc.), initiatives for self-regulation and the involvement of children in the establishment of a secure online environment and the creation of a knowledge base regarding the latest online technology trends and their consequences for the everyday life of children[209].

A constituent part of the programme is promotion of the *self-regulation of the internet industry*. As part of this, the most important social networks operating in Europe signed the "Safer Social Networking Principles for the EU"[210] in 2009. The principles provide for the user profiles of children to be automatically set as private and efficient mechanisms for reporting and deleting problematic content and inci-

---

[202] According to the EU Kids Online 2011 study, 27% of 9-12 year-olds on social networks provide an incorrect age and 38% of 9-12 year-olds have a social network profile. See EU Kids Online Final Report, September 2011, p. 18.

[203] Declaration of the European Parliament on protecting the dignity, security and privacy of children using the internet.

[204] Recommendation Rec(2006)12 to member states on empowering children in the new information and communications environment.

[205] Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment.

[206] The EU proposal for the General Data Protection Regulation, Communication (2012) final. For more information on the EU's efforts in relation to child protection, see the Commission's Communication on a European Strategy for a Better Internet for Children, COM(2012) 196 final, which contains comprehensive details of the Commission's requests and recommendations.

[207] See Art. 8 of the Proposal for an EU General Data Protection Regulation, COM(2012) 11 final.

[208] Decision 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the internet and other communication technologies, ABl. L 348 of 24.12.2008, p. 118–127.

[209] See http://europa.eu/legislation_summaries/information_society/internet/l24190d_de.htm and the Commission Communication "Interim evaluation of the multi-annual Union programme on protecting children using the internet and other communication technologies, Communication (2012) 33 final.

[210] Links to the "Safer Social Networking Principles" and the EU Commission's implementation reports are available at: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm. Another EU-level self-regulation agreement is the "CEO Coalition to make the Internet a better place for kids", which was established in December 2011. Basic documents and information about the agreement can be found at: http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm.

dents of contact. The programme also recommends the provision of easy to understand information regarding security and privacy on social networks and well-developed privacy settings, that contact with children by unknown persons be prevented and that the user profiles of children be made inaccessible via search engines.

#### 4.6.1.3 Legal status in Switzerland

The general statutory provisions described in the report, which can serve to protect against the risks of social networks, such as data protection law or the protection of personality rights under civil and criminal law, also protect children and young people. Instruments of protection against cyberbullying and cyberstalking (see Section 4.4.4.2.), identity theft (see Section 4.4.3.), pornography (see Section 4.5.2) as well as the health risks of social networks mentioned in the report (see para. 4.5.4) are particularly relevant to children.

In addition to these general rules, the Swiss legal system also contains a number of provisions that are specifically dedicated to the protection and promotion of children and young people. The special needs of children are therefore often expressed in the Federal Constitution and in various international agreements which are binding for Switzerland[211]. On a legislative and regulatory level, special protective provisions are provided for under criminal[212] and civil law[213], as well as under radio and television legislation[214], employment law[215] and under foodstuffs regulations (provision of alcohol)[216]. Federal lawmakers have also been active in the area of the advancement of young people[217].

To date there have been no other provisions for the protection of young persons under federal law that are specifically aimed at the regulation of social networks. However, certain provisions on the protection of children and young people also apply to social networks, e.g. the prohibition of advertising tobacco or alcohol to young people[218] or the prohibition of making pornography accessible to people below the age of 16.

Legal instruments alone are insufficient for the protection of children and young people. The actions of parents also play an important role. As part of their parental rights, they can determine their children's use of social networks and their personal data if the children are not capable of judgement as regards

---

[211] See Art. 11, 19, 41, 62, 67, 123b of the Federal Constitution. In relation to international treaties, see the Convention of 20 November 1989 on the Rights of the Child, CC 0.107, including its operational protocol or Übereinkommen Nr. 182 vom 17. Juni 1999 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit [Convention no. 182 of 17 June 1999 on the Prohibition of and Immediate Measures to Eliminate the Worst Forms of Child Labour], CC 0.822.728.2. The Convention of the Council of Europe on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25.10.2007 was approved by the Federal Council and Federal Assembly; see BBl 2012 7571 and BBl 2012 7653.

[212] Art. 5, 136, 187, 188, 195, 197, 213, 219, 220, 363f., 264f SCC; Federal Act of 20 June 2003 on the Criminal Law applicable to Juveniles (JCLA), CC 311.1; Swiss Juvenile Criminal Procedure Code of 20 March 2009 (JCrimPC), CC 312.1.

[213] Art. 296ff., 307-317 CC.

[214] Art. 5, 13 RTVA and Art. 4, 16 RTVO.

[215] Ordinance 5 of 28 September 2007 to the Employment Act - Youth Employment Protection Ordinance (EmpO 5), CC 822.115; Verordnung des WBF vom 4.12.2007 über gefährliche Arbeiten für Jugendliche (Ordinance of the EAER on Hazardous Work for Juveniles), CC 822.115.2.

[216] Art. 11 of the Ordinance of 23 November 2005 on Foodstuffs and Utility Articles (FoodO), CC 817.02.

[217] Bundesgesetz vom 30.September 2011 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFG) [Federal Act of 30 September 2011 on Fostering Extra-Curricular Work with Children and Young People], CC 446.1; Verordnung vom 17.Oktober 2012 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFV) [Ordinance of 17 October 2012 on Fostering Extra-Curricular Work with Children and Young People], CC 446.11; Verordnung vom 11. Juni 2010 über Massnahmen zum Schutz von Kindern und Jugendlichen sowie zur Stärkung der Kinderrechte [Ordinance of 11 June 2010 on Measures to Protect Children and Young People and to Improve Children's Rights], CC 311.039.1.

[218] Art. 18 of the Ordinance of 27 October 2004 on Tobacco Products and Smoking Goods with Tobacco Substitutes (TobO), CC 817.06 and Art. 4 of the FDHA Ordinance of 23 November 2005 on Alcoholic Beverages, CC 817.022.110.

their actions on social networks or if their judgement is at the very least doubtful. Whether a child is capable of judgement cannot be assessed abstractly, but only with respect to a specific act[219].

If the actions of a child capable of judgement affect their inviolable rights, the parental power of attorney is at its limits[220]. Children capable of judgement may exercise rights that they are entitled to for the sake of their person, unless the law requires the consent of their legal representative (Art. 19c CC). This is significant for activities on social networks because they regularly affect those rights of users to which they are entitled to for the sake of their person. Children capable of judgement therefore do not in principle require the consent of their legal representative in order to publish any personal data about themselves, e.g. photos, etc.., or self-generated content on social networks. The consent of a child capable of judgement is in principle also valid in the case of a violation of privacy (Art. 13 para. 1 SCC; Art. 28 para. 2 FADP).[221]

The national "Media Protection and Media Literacy for Young People" programme, which was launched by the Federal Council in 2010, aims to raise awareness amongst children and young people about the risks and opportunities online and to provide parents, teachers and other guardians with appropriate measures for supervising their internet activities, including social media. An example of a site that features measures for supporting parents, guardians and schools is http://www.jugendundmedien.ch/de.html (only available in German, French and Italian).

In a 2011 evaluation report on the FADP, the Federal Council presented the prospect of measures towards improved data protection of minors, which took account of the fact they are less aware than adults of the risks of processing of personal data.[222]

### 4.6.2 Employees

#### 4.6.2.1 Background

Internationally[223], but also in Switzerland[224], the risks of disclosing personal data in relation to future application processes are often discussed in relation to social networks. It is common knowledge that employers use internet search engines in recruitment processes in order to obtain information about potential future employees. Users are often insufficiently aware that once they post information on a platform it can, depending on the privacy settings, be retrieved by external search engines. In addition, employers can use third-party user profiles to access information that applicants disclose on social networks.

#### 4.6.2.2 Solutions in other countries and in international law

A draft legislation amendment to the German Federal Data Protection Act (BDSG) deals with the permissible scope of data collection prior to the establishment of an employment relationship (Bewerberdatenschutz [applicant data protection][225]. The draft prohibits employers from collecting data on job candidates on social networks, even if they are widely available (e.g. via external search engines). Professional networks (such as LinkedIn and Xing) are excluded from the rule. The development of

---

219 BSK-DSG, Bigler-Eggenberger Margrith, 4th ed., Basel 2010, Art. 16, p. 177f margin number 14.

220 BSK-ZGB, Schwenzer Ingeborg, 4th ed., Basel 2010, Art. 305, p. 1606 margin number 6.

221 Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 104 no. 70.

222 Report concerning the evaluation of the Federal Act on Data Protection of 09.12.2011, lit. 5.2.2 (BBl 2012 350)

223 See the Opinion of the European Economic and Social Committee on the "Responsible use of social networks and the prevention of related problems" (own-initiative opinion) 2012/C 351/07, p. 2, 7, 10.

224 "Schweizer Konzerne überprüfen Bewerber im Internet", Tagesanzeiger, 02.05.2011, http://www.tagesanzeiger.ch/leben/gesellschaft/Schweizer-Konzerne-ueberpruefen-Bewerber-im-Internet/story/17153295?dossier_id=510 (only available in German).

225 Draft legislation for the German Workplace Privacy Act, 17/4230.

the project remains to be seen, especially in the context of the current revision of European data protection law.

In February 2013 draft legislation was presented to the US Congress[226]; this prohibits employers, higher education institutions and local training centres from asking employees, job candidates, students and pupils for their username, password or other access to their accounts on social networks or to their personal e-mail accounts. It also states that data subjects may not be placed at any disadvantage if they refuse to disclose such information. In some US states, such as California, Maryland and Illinois, similar legal regulations are already in force[227].

#### 4.6.2.3 Legal status in Switzerland

In Switzerland, whether and to what extent employers may obtain information on job candidates via social media is not expressly regulated by law. Art. 328b of the Code of Obligations allows employers to process data regarding employees insofar as this relates to their suitability for employment or is required in order to perform the work contract. The Federal Supreme Court and a significant proportion of legal scholars consider that the provisions should apply to the application phase prior to the existence of an employment relationship, though legal opinion is also divided[228]. Thereby it follows from the wording of the standard that there is a substantive limit on the data that an employer may collect regarding a job candidate. Private, non-professional user profiles on social networks may contain certain information that provides information on the suitability of the employee. However, as a general rule private user profiles primarily contain information outside the scope of Art. 328b of the Code of Obligations, as data from the private sector only exceptionally falls under the concept of data on the suitability of employees[229]. Since employers inevitably view all the contents of a user profile when accessing the information, it is extremely doubtful whether they can have a right of access to the private network profile of job candidates based on Art. 328b of the Code of Obligations. This is why some legal scholars hold the view that general research on the internet using a search engine or on a social network that targets private individuals violates Art. 328b of the Code of Obligations[230].

If an employer accesses a private user profile by means of a prohibited act (e.g. a violation of Art. 143$^{bis}$ para. 1, Art. 179$^{novies}$ or Art. 181 SCC), they violate provisions under criminal law and the principle of legality of data processing (Art. 4 para. 1 FADP). The principles of good faith and visibility of data processing (Art. 4 para. 2 and 4 FADP) in turn prohibit secret data collection by employers. If a user profile is private and employers are not permitted to view it by its owner, it could be argued that a violation of Art. 12 para. 2 lit. b FADP exists if the employer accesses the profile. If an employer requests access to the private user profile of a job candidate, the voluntary nature of the candidate's consent may be fundamentally called into question, as they may fear disadvantages in the event of refusal.

It is questionable to what extent an employer's research into data that is generally accessible on the internet (Art. 12 para. 3 FADP) – for example public user profiles on social networks – is legally restricted. It is argued that a violation of personality rights exists if an employer uses a private network to

---

[226] Social Networking Online Protection Act of 06.02.2013, H.R.537.

[227] Kalifornien schützt private Online-Kommunikation vor Arbeitgebern und Unis, heise online, 02.10.2012, http://www.heise.de/newsticker/meldung/Kalifornien-schuetzt-private-Online-Kommunikation-vor-Arbeitgebern-und-Unis-1721503.html (only available in German) .

[228] See Decision of the Federal Supreme Court 2C_103/2008 of 30 June 2008, E. 6.2. In favour of the application of Art. 328b of the Code of Obligations to the application phase, see, Portmann Wolfgang, 5th ed., Basel 2011, Art. 328b, p. 1952 margin number 34ff and Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7th ed., Zurich 2012, Art. 328b, p. 580 no. 4. Against this see Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz, Zurich 2008, p. 731 no. 25.

[229] BSK-OR I, Portmann Wolfgang, 5th ed., Basel 2011, Art. 328b, p. 1947 margin number 8 and Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7th ed., Zurich 2012, Art. 328b, p. 581f no. 5.

[230] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter, 17.01.2011, p. 9f, margin number 65ff and Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7th ed., Zurich 2012, Art. 328b, p. 597 no. 10.

research information about a job candidate that is generally accessible and has no connection with the candidate's past or future professional activities. For a network such as Facebook where the focus is on private life, the data would therefore be subject to abuse by the employer if used for purposes which the data subject did not conceive of at the time of its publication[231]. In practice, however, it is almost impossible to prove whether an employer has viewed accessible data using a simple web search. In the case of professional social networks (e.g. XING and LinkedIn) it can be assumed that these have been deliberately created by the owner to give potential employers access to the data published[232]. Here too, however, a large amount of information is only accessible to members of the network.

A reasonable solution to the problems arising in this context requires platform operators to provide sufficient privacy settings, employers to strictly respect the privacy of job candidates, and users of social networks to be aware of their own responsibility in relation to the publication of data. In his comments on social networks, the Federal Data Protection and Information Commissioner recommends that prior to the publication of personal data, users consider whether they would wish to be faced with that data in a future job interview[233].

### 4.6.3 Persons with disabilities

#### 4.6.3.1 Background

The new information and communication technologies (ICT), including social networks, create new opportunities for people with disabilities to participate in social life and to obtain and exchange information. However, this requires that the internet and the information, communication and transaction services offered via the internet be designed accessibly (barrier-free).

#### 4.6.3.2 Solutions in other countries and in international law

Recommendations on an international level (Web Content Accessibility Guidelines (WCAG) 2.0 of the World Wide Web Consortium) aim to ensure the accessibility of ICT to users with disabilities[234]. Also, the Council of Europe Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services calls for the operators of social networks to guarantee the accessibility of services for people with disabilities.

#### 4.6.3.3 Legal status in Switzerland

In Switzerland, municipalities are subject to a legal obligation to offer accessible social media as part of their commitment to proportionality. This follows in principle from the prohibition of discrimination (Art. 8 para. 2 of the Federal Constitution) and, specifically for the federal government, from the Disability Discrimination Act[235], the scope of which includes services via the internet[236]. According to Art. 6 DDA, private providers of services that can in principle be used by anyone are only prevented from discriminating against disabled people on the basis of their disability. An obligation to provide accessible internet-based offerings cannot be derived from this.

---

[231] For example Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, margin number. 66ff.

[232] Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter 17.01.2011, margin number. 70f.

[233] See http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=de (only available in German, French and Italian)

[234] http://www.w3.org/TR/WCAG/.

[235] Federal Act of 13 December 2002 on the Elimination of Discrimination against People with Disabilities (DDA), CC 151.3.

[236] In relation to federal internet services, Article 10 of the Ordinance of 19 November 2003 on the Elimination of Discrimination against People with Disabilities (EPDO), CC 151.31 requires that all internet services and social media are to be made accessible for people with disabilities. The reference standard for federal websites is the P028 standard "Richtlinien des Bundes für die Gestaltung von barrierefreien Internetangeboten" [Federal Guidelines for the Design of Barrier-Free Internet Offerings]. See http://www.isb.admin.ch/themen/standards/alle/03237/ (only available in German and French).

Given the importance of social media in general, and in relation to the promotion of the participation of people with disabilities in society, ensuring accessible social media services is highly desirable. However, legislative measures at a national level would affect very few of the most popular social media services. It does, however, appear advisable to work with other measures and in association with key stakeholders towards observance of accessibility standards.

## 4.7 Amherd Postulate 12.3545 "Facebook Zugang für Kinder" [Facebook access for children]

Postulate 12.3545[237] commissioned the Federal Council to highlight what measures could protect children from the harmful effects of social media in Switzerland. As well as adjustments to legislation, the highlighting of measures to support parents, guardians and schools was also requested. She also considers it necessary to review whether it makes sense to link the profiles of children on Facebook to those of their parents and what options electronic identity cards such as the SuisseID would offer in this context. Surveys have shown that in Switzerland only very few children under 13 have set up a profile on a social networking platform. [238]

Facebook's idea of lowering the age limit for use to children under 13 years and to link the profiles of children under 13 with those of their parents may have a monetary background, because it would then be possible to reach a new target group, which would be of particular interest to the ever-growing games market that is advertised on Facebook. By linking children's profiles to those of their parents, Facebook may be able to obtain (implicit or explicit) parental consent in the case of conclusion of contract. On the other hand, it is conceivable that Facebook is trying to pre-empt the government regulation with its own initiative and thereby to make it obsolete.[239]

As has already been described in Section 4.6.1.3, the general statutory provisions, which can provide protection from the risks of social networks, also protect children and young people. In addition, numerous specific provisions for the protection and promotion of children and young people also apply in the case of social media.

Linking the profiles of children to those of their parents is problematic for several reasons. It presupposes that the parents have and maintain a profile on this social media platform. This would certainly be of benefit to the site concerned itself, but is likely to be rejected by many parents, who for various reasons do not wish to use the platform. Furthermore, linking the profiles of children and parents could result in a restriction of the personality rights of children capable of judgement.

In order for a standardised electronic proof of identity for age verification, etc. to be used on a social media platform, this platform would have to create the conditions in the system and verify each identity. Whether SuisseID would meet the requirements of Facebook in this context cannot currently be answered.

## 4.8 Attempt at an overall assessment of the current legal status

As far as the legislation for the various legal issues raised by social media presented in this chapter is concerned, the overall picture is extremely diverse. Generalisations are difficult. Generally speaking, it is possible to maintain on the basis of previous experience that the often broad provisions of applicable Swiss statutory law can, in the event of a dispute, be interpreted and applied in such a way that balanced solutions are possible. No major gaps are discernible in the law.

---

[237] http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20123545# (only available in German, French and Italian)

[238] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts, 2013, no. 1.4, p. 27; in Germany the problem seems to be pronounced, with an average age at first registration of 12.7 years: Caspar Johannes, Soziale Netzwerke und Einwilligung der Nutzer, in: digma 2013, p. 62.

[239] See e.g. http://online.wsj.com/article/SB10001424052702303506404577444711741019238.html#.

However, the current practice of Swiss courts and authorities is still limited. The question therefore arises as to whether existing legislation provides sufficient incentives for data subjects to actively defend their rights. There is room for improvement, for example, in various aspects of data protection (such as the resources of the FDPIC and the lack of a requirement for privacy-friendly default settings, see Section 4.3.1.5). Technical developments in particular could help to make the population more aware of existing legal claims.

In addition, there is still uncertainty in some areas as to whether the application of the general provisions to new legal issues in disputes that go to court will actually lead to satisfactory results in practice. This uncertainty is due not least to the fact that the practical enforcement of existing legal rights in the international environment of social platforms can be precarious.

# 5 Basic problem: Enforcement of the law

## 5.1 General

Chapter 4 examined whether existing Swiss legislation adequately covers (especially in the DSG, Civil Code, Criminal Code and Unfair Competition) the specific legal problems of social networks, with reference to individual issues.

A central problem, which is to be examined in greater detail at this point, is the implementation of existing legislation, as the party responsible for a violation of the law (e.g. the author of illegal posts on a social platform) often cannot be held accountable. It therefore raises the question of whether Swiss law sufficiently clarifies the responsibilities of the parties concerned.

Furthermore, operators of social media platforms are often international and national legislation is therefore at its limits.

## 5.2 Prosecution of authors of illegal entries on platforms

### 5.2.1 The problem of anonymity

As described in Chapter 4, posts on social platforms can infringe a large number of different provisions under criminal law (e.g. slander, pornography, racial discrimination, public incitement to commit a felony or act of violence) or civil law (e.g. the protection of personality rights). In legal reality, enforcement of these rules is often difficult. For example, the authors responsible for posts that may be illegal can only be held accountable if their identity is known. This is not always the case, as anonymous posts (or posts published under a pseudonym) in the comment column of blogs and social networks such as Facebook are commonplace. Definitive identification is difficult to impossible in such cases.

However, Swiss prosecuting authorities may pursue leads, e.g. via access to IP addresses, i.e. internet network addresses, which internet users do not normally have access to. They are usually recorded by the system operators when a user uses, for example, a social media platform or sends an e-mail. Whether this access is possible and permissible also depends on who operates the platform in question.

### 5.2.2 Anonymous posts on platforms of professional media representatives

The Swiss legal system has long since recognised that the motives underlying anonymous publication are not always reprehensible.[240] The Criminal Code even explicitly protects anonymous publication to a considerable extent. According to Art. 28a SCC and Art. 172 CrimPC, all persons professionally involved in the publication of information in the editorial section of periodical media may keep the author's identity secret. These persons and their assistants have the right to refuse to surrender any anonymous author's IP address if demanded by the law enforcement authorities. This right affects social platforms such as blogs if they are operated by professional journalists. For example, the Federal Supreme Court accepted the refusal of the SRG to submit to the Zuger Staatsanwaltschaft [Office of the Public Prosecutor of the Canton of Zug] the IP address of a person who had posted allegedly defamatory comments in the comment column of the SRG blog for the television show Alpenfestung.[241] If the author cannot be determined or cannot be prosecuted in Switzerland, it is possible that punishment of the responsible editor (or, alternatively, the person responsible for publication) may be considered for failure to prevent an illegal publication (Art. 322$^{bis}$ SCC).

### 5.2.3 Anonymous posts on other platforms

The situation is different in the case of operators of platforms who are not professional journalists. They may be required by the competent authorities to surrender the IP addresses of suspected per-

---

[240] cf. Decision of the Swiss Federal Supreme Court 55 II 94 E. 1 p. 98.

[241] Decision of the Swiss Federal Supreme Court 136 IV 145

sons. The relevant data should be stored in accordance with the Monitoring of Post and Telecommunications Act (MPTA; SR 780.1). The MPTA obliges all telecommunications and internet service providers (Art. 1 para. 2) to retain for six months all data required for identification of subscribers as well as traffic and billing data (Art. 15 para. 3) and to forward these to the Postal Service and Telecommunications Surveillance Service on request (Art. 15 para. 1). According to current practice and the French wording of Article 1, however, only internet access providers are subject to the obligation. Platform operators are only obliged to surrender existing data. According to Art. 22 para. 4 of the draft for a revised Federal Act on Surveillance of Post and Telecommunications [242] the Federal Council should be able to oblige providers of services which are based on telecommunications services and which enable one-way or multi-way communication (providers of secondary telecommunications services) to archive data, in the same way as telecommunications service providers. According to existing legislation, if a crime is committed via the internet, prosecuting authorities may reveal the identity of the subscriber of the connection and, for example, conduct a house search even without a court order. It was for this reason that in 2010, the Federal Supreme Court upheld the punishment of the operator of an internet platform for assisting offenders (Art. 305 SCC); the operator had, as a provider, deleted the IP addresses of the anonymous authors of allegedly defamatory comments in order to avoid criminal prosecution.[243]

However, enforcing the law is more difficult if the IP addresses are known only to the operator of a foreign platform that is not subject to the provisions of the MPTA. In this case, the Swiss authorities must rely on the cooperation of the foreign platform operator or take the arduous path of international mutual assistance in criminal matters. Foreign platform operators are sometimes not willing to delete content, but instead consent under certain circumstances and upon request to inform the prosecuting authorities of, for example, the IP address of the author of an illegal statement.

### 5.2.4 The issue of territorial jurisdiction

Particularly in the case of social media, practical problems in the prosecution of criminal offences arise from the fact that it is first necessary to determine which authority is responsible for prosecution. Only then can any necessary international mutual assistance in criminal matters (e.g. on Facebook) be provided and any criminal act be resolved. Since statements posted on international platforms can be retrieved anywhere, there is a risk that neither cantonal public prosecuting offices nor the Office of the Attorney General of Switzerland can be considered as responsible for initiating proceedings. For this reason, Art. 27 para. 2 CrimPC gives the Office of the Attorney General of Switzerland the option of initiating proceedings in the event of unclear jurisdiction. If the Office of the Attorney General of Switzerland applies this provision consistently, it is possible to prosecute offences on social platforms.

## 5.3 Responsibility of platform operators and providers

### 5.3.1 Solutions in other countries and in international law

Within the EU, the liability of internet service providers is specified by the special rules of the *E-Commerce Directive (ECD)*[244]: Art. 12 ECD lays down the principle that internet service providers and other pure "access providers" cannot be held responsible for the content of the information transmitted by them. According to Art. 14 ECD providers that store third-party content on their computers (hosting providers) are exempt from responsibility unless they are aware of illegal activity. If they are aware of illegal activity, they must remove, or disable access to, the content in question.

However, there is no obligation to monitor the information that is transmitted or stored or to actively investigate illegal content (Art. 15 ECD). The European Court of Justice (ECJ) has also recognised

---

[242] Federal Gazette 2013 2789

[243] Decision of the Federal Supreme Court 6B_766/2009 of 08.01.2010.

[244] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce ECD. L 178 of 17.7.2000, p. 1).

that providers should not be obliged to monitor in advance all the content that they store or make available. The ECJ has negated a general obligation to provide advanced filtering in the case of both access providers[245] and hosting providers[246].

If a provider does not remain limited to the automated processing of information entered by his customers, but instead selects or alters the information transmitted, the privilege of having no liability or duty to monitor granted under Art. 15 para. 1 ECD ceases to apply.[247] Such an active role cannot be assumed if the platform operator stores the services on its server, stipulates the modalities for its service, or receives compensation for this and provides its customers with general information. However, according to the ECJ it exists if the operator provides assistance, for example, in optimising the presentation or promotion of content. [248]

From a *human rights perspective* it is debatable whether and under what circumstances a platform operator may be prosecuted under civil law and ordered to pay compensation for personal suffering for unlawful illegal comments made by users (e.g. comments that infringe personality rights). The appeal of a convicted Estonian news portal operator for breach of freedom of expression (Art. 10 ECHR) has been pending at the European Court of Human Rights since 2009. [249]

### 5.3.2 Legal status in Switzerland

As in other countries, in Switzerland it is also undisputed that authors of illegal content (content providers) on social media are legally responsible if they can be identified and brought to trial. Unlike most European countries, Switzerland does not recognise any specific rules for the responsibility of other parties in the communication chain (e.g. the hosting and access providers). The general provisions for criminal and civil responsibility apply. Various critics have suggested that due to the decision not to adopt a special regulation, the legal status is not sufficiently defined. In 2001 the National Council and the Council of States demanded legally binding regulation and accepted a motion to this effect.

Subsequently, a "Network Crime" commission of experts was established. Based on their report, the Federal Council submitted a preliminary draft amendment of the Criminal Code (SCC) and the Military Criminal Code (MCC) for consultation in 2004. Explicit regulation of criminal responsibility for providers and search engine operators was welcomed, but there was disagreement about various details of the proposed regulation. In 2008, the Federal Council decided to waive regulation of criminal liability.

Subsequently, the Federal Council has again maintained that there is no reason to recommend adopting a special regulation of responsibility for access and hosting providers under either criminal or civil law (see Motion Riklin 09.4222 "Rechtliche Verantwortlichkeit von Internet-Providern" [Riklin Motion 09.4222 "Legal Responsibility of Internet Providers"] parlamentarische Initiative Hochreutener 08.418 "Mehr Rechtssicherheit bei Netzwerkkriminalität" [Hochreutner Parliamentary Initiative 08 418 "Greater Legal Certainty for Network Crime"] and lastly Interpellation Stöckli 12.4202 "Swisscom. Umgang mit urheberrechtlich geschützten Inhalten" [Stöckli Interpellation 12.4202 Swisscom. Dealing with Copyrighted Content].

- Under *criminal law* the Federal Council considers it possible to achieve appropriate solutions based on the criminal liability of the media (Art. 28 SCC) and the general provisions of perpetration and participation (Art. 24ff. SCC).

---

[245] CJEU Decision of 24.11.2011 SABAM / Scarlet Extended: Rs.C-70/10 (Order to access providers to filter and block file sharing in contravention of European law.

[246] CJEU Decision of 16.02.2012 SABAM / Netlog NV Rs. C 360/10 (No obligation for hosting providers to universally monitor the content stored on a social network platform and to set up a filter system in order to prevent the infringement of copyright)

[247] CJEU decision of 19.07.2011 L'Oréal / eBay Rs. C-324/09 Slg. I-6011 (liability for providers with an "active role")

[248] CJEU decision of 19.07.2011. L'Oréal / eBay, Rs. C-324/09, Slg. I-6011 margin number 115f

[249] Appeal no. 64569/09 "Delfi AS vs. Estonia"; the matter was submitted by the Court to the Government of Estonia for its opinion on 11.2.2011.

- With regard to responsibility under *civil law*, providers are liable according to the same principles as providers of other services. They are obliged to provide compensation in accordance with the Code of Obligations if they unlawfully cause loss or damage to another, whether wilfully or negligently (Art. 41 para. 1 of the Code of Obligations).[250]

To date the responsibility of social media platform operators, which do not fit into the usual category of provider, has not been clarified.[251] Platform operators generally play a more active role than pure hosting providers, which only allow their customers to automatically upload information on their web server. They have a closer connection to the communicated content than those hosting providers that only provide storage space. Platform operators determine the rules for the design, scope and content of user-generated content. Unlike traditional hosting providers, they are often able to exercise a monitoring role and, if necessary, take action against problematic content. Waiving a certain level of filtering using at least randomly sampled control measures or timely action against illegal content could in this case be more likely to have consequences under criminal and civil law. To date attempts to outline the scope of their duties by the judiciary and jurisprudence[252] have been rudimentary at best.

It is therefore debatable whether and to what extent platform operators fall under the special rules governing criminal liability of the media (Art. 28 SCC) and whether a subsidiary responsibility for the failure to prevent a criminal publication (Art. 322$^{bis}$ SCC) applies in the case of crimes of expression. One of the problems is the fact that many platforms contain both private content and content that is directed at a wide audience. The current law on criminal liability of the media does not adequately recognise such hybrid forms. Unlike periodical publishers, broadcasters or operators of individual websites, social network operators are not media companies in the traditional sense of the word.

Legal literature maintains that the special standard for criminal liability of the media (Art. 28 SCC), which derives from the age of the printing press, no longer satisfies the requirements of today's online age. Its scope is unclear in the case of various crimes (e.g. soft-core pornography) and especially in the case of publication in various mass-media internet applications. Legal literature is of the opinion that limits on the extent of criminal culpability should therefore be clarified by means of revision of legislation.[253]

The Federal Council is aware that not only providers, customers and authorities, but also the judiciary benefit from clear legal rules. However, given the large number of players and their different needs and problems, every conceivable bill on the responsibility of internet providers and the prosecution of infringements on the internet presents the challenge of finding a solution to satisfy everyone's requirements. This presents a danger not only of overregulation, but also of underregulation.

In its response to current parliamentary motions (Motion Riklin 13.3215 "Rechtliche Verantwortlichkeit von Internet-Providern regeln" [Riklin Motion 13.3215 "Regulate the Legal Responsibility of Internet Providers" and Frage Glättli 13.5059 "Haftbarkeit von Hosting-Providern, Blog- und Forenbetreibern" [Glättli Question 13.5059 "Liability of Hosting Providers, Blog and Forum Operators"]), the Federal Council recognised that legislative action may be necessary with regard to civil law: the Federal Court has now dealt with the issue of civil responsibility of hosting providers for illegal content (content that infringes personality rights).[254] It has rejected a liability privilege for deletion and determination re-

---

[250] Stellungnahme des Bundesrates vom 05.03.2010 zur Motion 09.4222 – Rechtliche Verantwortlichkeit von Internet-Providern [Opinion of the Federal Council of 05.03.2010 on Motion 09.4222 - Legal Responsibility of Internet Providers].

[251] Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: medialex 2009, p. 21f.

[252] cf. Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: medialex 2009, p. 19ff.

[253] Christian Schwarzenegger, Der Anwendungsbereich des Medienstrafrechts (Art. 28, 322$^{bis}$ SCC), in: Cavallo and others. (ed.), FS-Donatsch, Zurich 2012, p. 187

[254] Decision 5A_792/2011 of 14 January 2013.

quirements in the case of a provider that retains third-party blogs for retrieval on its own server. It is of the opinion that Switzerland has not to date adopted any special rules, which is why the general rules of Art. 28 CC are applicable.[255] It also believes that it is not the role of the judiciary, but of the legislature to correct any adverse consequences of this legal status.[256] The Federal Court referred expressly to the present report, which was then in preparation.

Current case law suggests that the judiciary feels the general rules on civil responsibility are inadequate and is hoping for clarification in this area by the legislature. The statements of the judiciary and jurisprudence[257] and foreign developments [258] suggest that further consideration of legislative action in civil law is required. The Federal Council is prepared to initiate appropriate action (cf. Section 7.2.4).

## 5.4 Deletions and blocking orders

### 5.4.1 Deleting problematic content on platforms

In the case of illegal content on a social media platforms, if there is a link to Switzerland, the competent law enforcement authority may take steps to delete it. One of the options for a legal basis for deletion is an approach based on the provision for confiscation (Art. 263 CrimPC), if the content in question is used as evidence or is otherwise included during criminal proceedings. Based on Art. 13e of the Federal Act on Measures to Safeguard Internal Security (SR 120), in the case of distribution of violent propaganda via the internet, fedpol can also order the deletion of the site if the propaganda is on a Swiss server. If the propaganda material is on a foreign server, fedpol may advise Swiss providers to block the site in question. In relation to specific breaches of advertising regulations (for example in the Alcohol Act) the competent administrative authority (e.g. the Swiss Alcohol Board) can furthermore enforce the law via a decision in accordance with administrative law. Here too, enforcement of the legislation may be associated with difficulties precisely with regard to statements originating from abroad.

During the deletion process it should be kept in mind that only illegal content be removed and legal statements should continue to be accessible if possible, otherwise it is likely that there will be an exaggerated and therefore disproportionate restriction on freedom of expression (Art. 16 of the Federal Constitution - see also Section 4.2.2).

In the experience of CYCO it is simple to delete illegal content on those social platforms that take initiatives on their own after a relevant report is made. This includes, for example, Facebook. Operators of social network platforms based in Switzerland have not yet created self-regulation that is applicable to the industry as a whole. To date German platform operators[259], for example, have also foregone self–regulation due to cross-border contexts.

However, in relation to hosting providers there are attempts at self-regulation of the industry that provide platform operators (and other interested parties) storage space for the automated linking of their services. After three years of preparation a number of large Swiss hosting providers[260] developed a

---

[255] Decision 5A_792/2011 14 January 2013, E. 6.1.

[256] Decision 5A_792/2011 14 January 2013, E. 6.3.

[257] Kernen Alexander, Volle Verantwortlichkeit des Host Providers für persönlichkeitsverletzende Handlungen seines Kunden, in: Jusletter, 4 March 2013, margin number 20ff.; Bühlmann Lukas, Blog-Hoster sind mitverantwortlich für persönlichkeitsverletzende Blogbeiträge, in: Digitaler Rechtsprechungs-Kommentar Weblaw, 13 March 2013, margin number 10f.; Schoch Nik / Schüepp Michael, Provider-Haftung "de près ou de loin?", in: Jusletter, 13 May 2013, margin number 43ff; Hürlimann Daniel, Replik: Das Leistungsschutzrecht für Presseverlage, in: Jusletter, 13 May 2013, fn. 30.

[258] For example, the above-mentioned (fn. # 250) Application no. 64569/09 "Delfi AS vs. Estonia", which was filed with the ECtHR, on the obligation of a news portal to pay compensation for personal suffering for automatically linking unlawful illegal content (e.g. comments that infringe personality rights).

[259] http://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html (only available in German).

[260] According to simsa, these include the largest Swiss hosting providers, namely Cyon, Green, host Point, Metanet, Nine, Swisscom and Webland.

code of conduct[261] under the direction of the industry association simsa in 2013. This seeks to clarify their role in the prosecution of illegal content on the internet. This includes offences in relation to pornography, representation of acts of violence, racism and libel, but also a violation of copyright and moral rights. If the operator of a website or social platform does not allow identification or does not respond to inquiries and if a criminal charge does not seem likely to be successful, the data subject may submit their complaint to the hosting provider. According to the code of conduct, the hosting provider should forward the allegations to the operator of the offending website (or platform) and instruct them to clarify the allegations and, where appropriate, remove illegal content. In "clear cases", the hosting provider can also temporarily block access to the website concerned in accordance with the code of conduct.

German studies have shown that self-regulation models (and government regulated self-regulation) have certain advantages over legislative regulation, but that they operate in a complex and unstable manner. Self-regulation is really at its limits when it comes to the behaviour of external service providers that do not belong to the industry association (e.g. foreign service providers).[262]

### 5.4.2 Blocking access to problematic content via access providers

If prompt deletion of problematic content on the affected (usually foreign) social media platform is not possible, blocking access may be considered. In relation to child pornography and child abuse, CYCO provides Swiss providers with a list of links to foreign websites that have clearly illegal content are still available despite removal requests to foreign authorities. Based on their general terms and conditions, providers should ensure that a prohibition notice from CYCO appears instead of the prohibited content. This type of voluntary cooperation between public authorities and the private sector has proved useful. Thanks to this collaboration, hundreds of thousands of attempts to call up websites with illegal content are blocked by internet service providers every year, thereby ensuring the rights of victims to the greatest extent possible.

Furthermore, Swiss law prosecuting authorities have sporadically imposed such blocks in the past. One example is the imposition of a block by an examining magistrate for the canton of Vaud on the website "Appel au peuple" due to defamatory content.[263] Legal literature has voiced criticism of such injunctions, claiming that they do not have a clear legal basis in Swiss statutory law. [264]

In the context of restrictive measures, possible collateral damage for legal content that is also blocked should be kept in mind. If access to certain domain names is made impossible, any legal and desirable service offers will cease to be available at this domain name.[265] In a Turkish case[266] in late 2012, the European Court of Human Rights rejected the blocking of the entire Google Sites platform in response to a single problematic site. Such restrictive measures require a sufficiently precise legal basis. According to the Court, the legal framework must be strictly outlined and the control of such restrictive measures designed in a particularly effective manner by the national judiciary in order to prevent arbitrariness.

---

[261] Code of conduct hosting (CCH); http://static.simsa.ch/1362151411/130201_simsa_cch_public_web.pdf (only available in German).

[262] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts, 2013, no. 2.2.2.1.4, p. 45.

[263] cf. the facts of the Decision of the Federal Supreme Court 1B_242/2009 of 21.10.2009.

[264] Schwarzenegger Christian, Sperrverfügungen gegen Access-Provider - über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Arter Oliver/Jörg Florian (eds.), Internet-Recht und Electronic Commerce Law, Bern 2003, p. 249f.

[265] Rosenthal David, Internet-Provider-Haftung – ein Sonderfall? in: Peter Jung (ed.), Aktuelle Entwicklungen im Haftungsrecht, Bern/Zurich/Basel/Geneva, 2007, p. 158.

[266] ECtHR Judgement "Ahmet Yildirim vs Turkey" (Case no. 3111/2010) of 18.12.2012 on the blocking of the platform Google Sites in violation of the ECHR.

In view of the existing legal basis and the successful cooperation between authorities and internet service providers, the Federal Council denied the need for the creation of a legal basis in its response to the Anfrage Schwaab (12.1128 – Zugang zu Inhalten im Internet. Grundsatz "Löschen statt Sperren [Schwaab Query 12.1128 - Access to Content on the Internet. The "Blocking-Not-Deleting" Principle]).

## 5.5 Problems of law enforcement in a cross-border context

The enforcement of existing Swiss legislation on social networks is made significantly more difficult by the fact that most platform operators are foreign and communication is regularly cross-border. In many cases, Swiss law has a provision for the problems associated with social media. It is possible that Swiss law could be applicable to cross-border issues. However, even if there is a final judgement by a Swiss court, there is no guarantee that this will also be implemented in other countries.

### 5.5.1 Law enforcement by investigating and prosecuting authorities

#### 5.5.1.1 International cooperation

In practice, law enforcement depends largely on the willingness of the (foreign) platform operator to cooperate. This willingness can be encouraged through the intervention of prosecuting authorities. In this way certain operators of social media platforms have created offices to which foreign authorities may put their concerns without having to resort to legal remedies. [267]

In the event of a dispute, the prosecuting authorities have to proceed in accordance with the rules of international mutual assistance in criminal matters, which might significantly delay prosecution. Given the many cross-border issues, there are often no alternatives to international cooperation between investigating authorities. [268] For example, if a criminal prosecution is initiated in a foreign country (e.g. hacking or data theft), it becomes easier for the Swiss prosecuting authorities to exchange information with their foreign counterparts.

CYCO reports that there has been a marked increase in the exchange of criminal information since the European Convention on Cybercrime (Cybercrime Convention, CCC) entered into force on 1 January 2012. [269] CYCO forwards information concerning illegal content on foreign servers to the relevant authorities via Interpol or Europol in order that the countries concerned can delete the content and begin prosecution in line with its legal basis. Although this content, which is prohibited under Swiss law, can be retrieved in Switzerland, CYCO has no direct influence on the deletion or blocking of illegal content in other countries.

#### 5.5.1.2 Limits of measures against foreign television broadcasts

International legal boundaries are applied to any possible blocking measures if they affect actual television programme services. According to the European Convention on Transfrontier Television (ECTT), which is binding for Switzerland, the transmitting state is in principle solely responsible.

The transmission of actual television programmes (i.e. simultaneous or "streaming" transmission of integral audiovisual content that is collated by the broadcaster in a manner similar to that of programme services) via social media platforms is still rare. What is much more common on social networks is the provision of individual audiovisual content for retrieval ("video-on-demand" or "non-linear television). For such services, EU law also provides for the state of transmission (or the country of origin) principle. The relevant legislation, the Audiovisual Media Services Directive (2010/13/EU), is

---

[267] In relation to official requests, Facebook states " We scrutinise each request for legal sufficiency under our terms and the strict letter of the law". For the first half of 2013 Facebook stated that the company provided data about specific users in 13 percent of Swiss requests. https://www.Facebook.com/about/government_requests

[268] Hans Bredow-Institut, Entwicklungs- und Nutzungstrends im Bereich der digitalen Medien und damit verbundene Herausforderungen an den Jugendmedienschutz, Entwurf des Endberichts, 2013, no. 2.2.2.2.1, p. 48.

[269] CYCO Annual Report 2012, no. 4 p. 20

not yet binding for Switzerland in relation to on-demand services. However, it cannot be ruled out that it might be in future.

### 5.5.2 Law enforcement by private individuals (e.g. to protect their personality rights)

In the case of problematic posts on social platforms, enforcing the law is difficult not only for the authorities but also, for example, for private individuals whose personality rights may have been violated by the publication of images or text. [270] If a user posts illegal content on a social media platform that the data subject wishes to be removed, the following procedure is necessary in practice: first, contact the author of the violation, then contact the platform operator, and finally, if necessary, review and initiate legal proceedings. Such an approach has proved successful in a number of cases.

#### 5.5.2.1 Applicable Law

In the first instance the applicable law in case of dispute is of great significance to the enforcement of law by private individuals. In their choice of law clauses the conditions of use of social media usually refer to the national or local law of the provider (e.g. California law), which is typically not based in Switzerland, even if the provider's subsidiaries have a presence in the country. The conditions of use usually stipulate the place of jurisdiction as the national or federal court where the operator is registered. However, this begs the question of the extent to which such choice of law and jurisdiction clauses are enforceable. The mandatory provisions of Swiss private international law stipulate the following:

Choice of law can only apply where a contract has been concluded. Although a user registration will typically suffice to satisfy this condition, insofar as a platform violates the rights of "non-users", the provider will not be able to refer to the choice of law in its conditions of use as a defence. For example, if it violates the personality rights of a person, the latter will take legal action before a Swiss court in accordance with the general rules for determining jurisdiction for tort claims in an international context, and can apply Swiss law based on the general rules of private international law. The same applies to violations of the unfair competition legislation. In order to apply Swiss law an effect on the Swiss market is necessary: it is usually sufficient if the activities in question are directed by a provider at parties including Swiss customers (Art. 136 IPRG[271]). Foreign providers of social media platforms for Swiss customers will therefore have to adhere to the provisions of unfair competition legislation (including Art. 8 UCA, which regulates the permissible contents of T&Cs), no matter what their conditions of use stipulate. The same applies to data protection: registered users can also ask a Swiss court to judge breaches of data protection law according to the FADP, if they so wish (Art. 139 IPRG), irrespective of the conditions of use or any choice of foreign law contained therein.

Secondly, clauses on jurisdiction and choice of law in the conditions of use are not applicable where the stipulation of international private law, including any international treaty, concerning the jurisdiction and contract law applicable between the user and provider is mandatory or semi-mandatory. It does this with regard to the protection of consumers in the case of contracts that such a consumer concludes in Switzerland via a website, even if the provider is in a foreign country. In such cases, any consumer domiciled in Switzerland will in principle assert their rights against the provider before a Swiss court (Art. 15 para. 1 lit. c LugC[272]; Art. 114 para. 1 lit. a IPRG), which in turn will apply Swiss (contract) law (Art. 120 IPRG).

---

[270] The remarks made in Section 5.5.2 are based on a text by David Rosenthal, Lecturer in Information and Telecommunication Law at the University of Basel, commissioned by the Federal Office of Communications in February 2013. A full version of the text can be found at: http://www.infosociety.admin.ch. (only available in German)

[271] Federal Act of 18 December 1987 on International Private Law (IPRG), CC 291

[272] Convention of 30 October 2007 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters (new LugC), CC 0.275.12

#### 5.5.2.2 Recognition and enforceability of claims

In practice, however, the applicability of Swiss law and the competence of Swiss courts with regard to the relationship between the user and the provider cannot itself guarantee that it will be possible to enforce claims against foreign (particularly American) social media providers. This would require recognition and enforcement proceedings to be initiated by the data subject before the courts in the country of the provider concerned. Even if the recognition and enforcement of a Swiss court judgement is in principle possible in another country, and somewhat simplified by international agreements,[273], the proceedings in question often offer the provider (another) opportunity for example to defend itself against the jurisdiction of the Swiss court (which will typically have decided against the agreed jurisdiction clause). This may prevent or at least delay recognition and enforcement. The options which the provider has in this context also depend under certain circumstances on foreign law. Sometimes it may be preferable for data subjects to assert their claims locally and waive the protection of Swiss law.

However, in both scenarios the costs associated with litigation deter many data subjects. Overall, legal disputes arising from the relationship between social network platform users and providers are rare in Switzerland.

There are also foreign social media platforms that "voluntarily" (i.e. without enforcement proceedings abroad) accept and comply with decisions made against them in Switzerland. In their conditions of use, most operators prohibit not only "illegal" content (which of course covers content that violates the FADP), but slander of other users or third parties in general; some go even further than what the law prohibits (see Section 4.2.2). Larger operators have their own teams that deal with such complaints, because they receive many of them every day.

Many operators do not wish to make a legal assessment themselves, but instead require the enforceable decision of a competent authority in the country concerned. If such a decision is presented to the operator, they block the content that is specifically designated and recognized as illegal, even if the decision is not made against the operator itself and without the need for international mutual assistance in criminal matters. In such cases, although the data subject must take legal action, they can limit their expense, because it is sufficient to initiate proceedings in Switzerland. There are also other options in these cases; these are usually dependent on two questions: First, has there been any conduct that could be considered a criminal offence (a mere breach of privacy may be illegal, but is usually not relevant, i.e. punishable, under criminal law but can "only" be pursued in a civil court suit); and second, has the author of the damaging statement been definitively identified?

If personality rights have been infringed by an unknown author, it is not possible to take legal action "against persons unknown" in a Swiss civil court. In such cases, it is necessary to take formal legal action against the operator of the platform, unless another person has played a role in infringement of personality rights (e.g. the person responsible for the site on which the statement infringing personality rights appeared) and unless the operator is willing to name the responsible person. In Switzerland the protection of personality rights offers the option of civil legal action against anyone who "participates" in an infringement of personality rights. According to the prevailing opinion, the operator of a social media platform (e.g. a blog) is included, even if they only play a secondary role in relation to the publication[274]. According to the prevailing interpretation, this includes operators of social media platforms. Unlike a cooperative operator, who nevertheless prefers to have a court decision or mandate from an authority before blocking content, action against an awkward operator is, in practice, usually only really useful if they are based in Switzerland or a country where quick and simple recognition and enforcement of a Swiss decision is possible.

---

[273] e.g. compared to the EU and EFTA countries, the above mentioned Lugano Convention concerning the jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

[274] cf. FSC 5A_792/2011 of 14.1.2013 E. 6.2 (for the operator of the Tribune de Genève blog platform); in agreement cf. Fanti Sébastien, Remarques, in: medialex 2013, p. 80.

The data subject may also take legal action in the foreign country in which the operator is based. This need not necessarily be more expensive than proceedings before a Swiss court, but is not usually possible without legal representation and the attendant costs.

#### 5.5.2.3 Preventive legal protection

Current law provides measures including demands to deletion, elimination, determination and satisfaction and damages to protect personality rights. Given the risk of the rapid transmission of statements that violate personality rights, there is a particular need for rapid legal protection. In practice, it is common for the court to request preliminary measures. They are intended to prevent infringing content remaining online while normal court proceedings are ongoing; it can take several years to go through all instances. The removal of content or a temporary publication ban is therefore issued at the beginning of, or even prior to, the proceedings. This generally happens without delay in the case of measures pronounced provisionally, based solely on the observations of the applicant, without consulting other affected persons or third parties. In the case of other precautionary measures a hearing takes place and can be expected to take several weeks.

In short, within the context of proceedings for preventive action, a decision is made as to whether action is required urgently, whether it is likely to be successful (e.g. whether certain content is actually illegal), whether the request for provisional measures is justifiable for the duration of the proceedings with regard to consequences for the defendant (e.g. what disadvantages could the provisional blocking or deletion present for the defendant), and whether the plaintiff might suffer any disadvantage that could not be easily rectified (i.e. by means of money). If preliminary measures have been ordered, the claimant must take action against the defendant within a certain time limit, otherwise the measure becomes invalid.

The enforcement of preventative measures is complicated in the international context and is often possible only subject to some delay. Thus some temporary injunctions are excluded from the scope of the Lugano Convention,[275] so that they do not benefit from the facilitated recognition and enforcement mechanism of this Convention. It can sometimes take months from the issuing of preventative measures to their enforcement abroad.[276]

#### 5.5.2.4 Other aspects of effective protection of private interests

In practice, effective protection of private interests cannot be realised by means of judicial intervention alone. Even after the removal of content from a platform it may be necessary to clean up search engines because the search continues to produce a hit (and the previous version of the page may be accessible on the cache unless caching is disabled by the owner of the site). In this instance, help is offered by a commonly offered special feature that allows users to command search engine robots to rescan a specific page again in advance or remove it from the search index (the internet address of the website concerned must be entered in order to do this).

Another problem is that once published, content (e.g. videos) is acted upon by other users, who can in turn redistribute it ("viral effect"). This can ultimately make it impossible for the data subject to effectively suppress undesired publication, even if legal rights and instruments exist.

In certain situations it may be useful for a slandered person to become actively engaged and defend their reputation. This can encourage the platform operator to act resolutely against certain illegal content. One reason for this is the fact that operators do not usually have any interest in negative publicity or a large number of angry users and do not wish to be portrayed as platforms for cyberbullying or character assassination. In the face of public pressure, they therefore quickly remove such content in

---

[275] ECJ judgment of 21.5.1980 Denilauler / Couchet, Rs. (C-125/79: precautionary measures which can be enforced without summons or prior delivery are not capable of circulation).

[276] For an illustrative example, see Schneider-Marfels Karl Jascha, Facebook, Twitter & co: "Imperium in imperio", in: Jusletter of 20 February 2012.

order to protect their own reputation, whereas they may perhaps deal with cases that attract no public attention more slowly and with less urgency. Conversely, public attention can increase the impact on the victim of an attack and can lead to the transmission of content spiralling out of control.

# 6 Other legal issues not covered in depth in this report

In addition to the issues mentioned in Chap. 4 and 5, social media throws up a number of other questions from a number of different angles. It is not possible to discuss all of these in depth here; instead they will be mentioned briefly in the following.

## 6.1 Copyright enforcement in social media

The enforcement, partially perceived as precarious, of copyright and related rights in the online age also concerns social media platforms. Measures to combat copyright infringement on the internet (e.g. by the exchange of unlicensed music, film and text files by means of file sharing and streaming) are currently being discussed within the framework of the AGUR12 working group set up by the Federal Department of Justice and Police. At meetings held to date, the members agreed that business models based on the infringement of Swiss or foreign copyright must be combated effectively. Here, the infrastructure operators (providers) which operate such business models must provide assistance in terms of what is reasonable, technically feasible and legally permitted..[277]

In addition, since 2012 the State Secretariat for Economic Affairs has initiated a round table which is intended to examine, in the framework of the existing legislation, how copyright infringements on the internet can be identified and prosecuted.

## 6.2 Competition problems of social media

This report discusses individual aspects of the dominant position of certain social media platforms and their impact on the interests of customers (lock-in effect, right of access to (dominant) social media platforms).

Furthermore, it is possible to deal with abuse of a dominant market position in both the social media sector and other sectors using the usual instruments of general competition law (especially the Cartel Act).

## 6.3 Social media services of broadcasters

Like other media companies, radio and television broadcasters have an increasing presence on social media. In principle the law presents no special barrier to their activities. To date, legislators have deliberately not adopted any regulation to this end within the framework of the RTVA.

However, an exception applies to the SRG. The SRG's social media presence is financed by reception fees and is part of its other news and information offerings, the scope of which is regulated in the licence in accordance with Art. 25 para 3 lit. a RTVA. According to the Federal Council's proposal, responsibilities for problematic statements should be regulated to a greater degree and regulatory responsibilities clarified. The Federal Council's intention is to ensure on a legal level that content generated by SRG editors – but not user-generated content – complies with certain minimum requirements (respect for human dignity, fundamental rights, the prohibition of representation of acts of violence, protection of young people, and in the case of certain services, factual accuracy and the diversity obligation). The Federal Council suggests that these minimum requirements also apply to entries of editors on blogs and forums.[278]

## 6.4 Communication between criminals on closed networks

The focus of this report is on social networks that are characterised by their accessibility and availability to the public, and the resulting problems. Specific problems arise in the case of clandestine com-

---

[277] Further information is available at: https://www.ige.ch/en/copyright/agur12.html

[278] Dispatch on the Amendment to the Federal Act of 29 May 2013 on Radio and Television (RTVA), no. 2.2 BBl 2013 5017

munication for the purpose of committing crimes, such as the exchange of pornography on P2P networks.[279]

They are sometimes countered by covert investigations in accordance with applicable law. For example, having regard to the police ordinance of the Canton of Schwyz, employees of the Cybercrime Coordination Unit Switzerland (CYCO) act as covert preliminary investigators against paedophile perpetrators in online chatrooms, online platforms and private P2P file-sharing networks.[280] CYCO also monitors P2P networks to detect paedosexual offences.[281]

## 6.5 IT espionage (monitoring by foreign secret services or private individuals)

The monitoring of online communications by intelligence services assumed greater public awareness in connection with the revelations by Edward Snowden which became known in 2013 (he is a former employee of the U.S. foreign intelligence service - the National Security Agency, NSA).[282] By using interfaces, the NSA can also monitor, collect and store the content of social media platforms.

The phenomenon of IT espionage - either by foreign intelligence agencies or individuals - is not primarily a problem of social platforms, but also affects exclusively private online communications even more. In its response to the Eichenberger Interpellation 13. 3358 Cyberspionage. Einschätzung und Strategie[283] of 20.06.2013 [Eichenberger Cyberespionage. Estimates and Strategies], the Federal Council referred to the "Strategie zum Schutz der Schweiz vor Cyber-Risiken" [National Cyber Strategy, NCS] of 27 June 2012 and the accompanying implementation plan. The NCS implementation plan adopted on 15 May 2013[284] relates to the 16 measures envisaged in the strategy. By means of the strategy, the Federal Council is pursuing the goals of early detection of cyber threats, increasing the resilience of critical infrastructures, reducing cyber risks and dealing with incidents.

In reply to the Schwaab Interpellation 13.3033 of 06.03.2013, "Wie können Personendaten von Schweizer Bürgerinnen und Bürgern in den Händen amerikanischer Unternehmen geschützt werden[285]" [How can the personal data of Swiss citizens in the hands of American companies be protected?] the Federal Council commented on various issues of Swiss legislation and practice in relation to the demands for personal data of citizens of third countries in the data cloud by the US authorities. In addition to the required responsibility of every individual in relation to the handling of personal data, the Federal Council highlights the Federal Government's awareness-raising programme "Jugend und Medien" [Young People and Media][286] as well as the advisory function of the FDPIC. In addition to comments on contract law and the possible applicability of the IPRG[287] and the Lugano Convention,[288] the Federal Council refers to the ongoing work on the revision of the FADP[289], where among other things it should be ascertained whether the applicable law in this area is adequate.

---

279 In 2012, CYCO was as a result of active monitoring able to identify 417 persons involved in the exchange of child pornography; cf. CYCO Annual Report 2012, p. 1.

280 CYCO Annual Report 2012, p. 13.

281 cf. Lentjes Meili Christiane, Präventiv oder Repressiv? Das Verwirrspiel um verdeckte polizeiliche Operationen, in: Festschrift Donatsch, Zurich 2012, p. 437ff.

282 Since at least 2007, the United States has monitored telecommunications and in particular the internet on a large scale globally and regardless of whether any suspicion exists, and has stored the resulting data.

283 http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133558.

284 http://www.isb.admin.ch/themen/01709/01711/index.html?lang=en

285 http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20133033.

286 http://www.bsv.admin.ch/themen/kinder_jugend_alter/00071/03045/

287 Federal Act of 18 December 1987 on International Private Law (IPRG), CC 291

288 CC 0.275.12.

289 CC 235.1.

# 7 Recommendations for action

The following presents recommendations on how to counter the problems identified in Chap. 4 and 5. As stated, substantive Swiss law is often sufficient and in practice many problems cannot be solved with legal instruments alone – and perhaps not even primarily with legal instruments. In addition to legal aspects, aspects such as information and awareness-raising will therefore also be addressed.

## 7.1 Need for the creation of new legislation

### 7.1.1 Background: Danger of overregulation

As shown above, it is from many angles conceivable – though not certain – that the wording of current legislation and its (legal) application in individual disputes may not allow satisfactory responses to the issues raised by social media. It cannot be ruled out that selective regulation will be required. However, legislative activism and overregulation is generally discouraged. As in other areas subject to rapid change, there is the risk that hasty intervention (to some extent an adoption of regulation in advance) can cause unintended consequences.

In each case it should carefully be considered whether existing self-regulation mechanisms are sufficient (e.g. the above-mentioned (Section 5.4.1) code of conduct for Swiss-based hosting providers that are part of the simsa association, but also the conditions of use of individual foreign platforms such as Facebook or Twitter).

### 7.1.2 International aspects restrict national regulatory discretion

The pronounced cross-border contexts also suggest that it is wise to limit Swiss legislation. Many problems cannot be appropriately countered with regulations by a single country. As mentioned, many of the heavily used platforms in Switzerland have their headquarters abroad.

What is needed is not expensive domestic regulatory activities with limited effectiveness, but enhanced international efforts: the Council of Europe is right to point out that regulatory measures taken in one jurisdiction may affect access to and the use of the internet in other jurisdictions, and have a significant negative impact on continued internet efficiency[290]. Consequently, the cross-border exchange of information on the internet requires engagement on a multilateral level. In particular, this includes situations that involve different legal systems, which is occurring with increasing frequency as cross-border platforms such as social networks develop, or with the rise of cloud computing[291].

### 7.1.3 Coherence of the legal system as a whole should be considered

Nevertheless, if a need to regulate certain individual areas on a national level is recognised, the coherence of the legal system as a whole should always be kept in mind. Many problematic aspects related to social media also apply to other areas of life: the right to be forgotten and the lack of control over one's own data is also an issue in other forms of online communication and everyday life in general[292], the protection of personality rights is also threatened by statements made and disseminated by conventional mass media (press and broadcasting), the protection of young people is also threatened by computer games, pornography is not limited to the internet, etc.

This means that general legislation that is not tailored to social media (e.g. the Criminal Code, Civil Code or Data Protection Act) already exists for many issues. Legislation that is isolated and tailored solely to the phenomenon of social networking runs the risk of fragmentation and tends to run counter to the coherence of the legal system. It is therefore generally advisable to seek any further develop-

---

[290] See, for example, the Declaration on the Principles of Internet Governance and Recommendation CM/Rec(2011) 8 on the protection and promotion of the universality, integrity and openness of the internet.

[291] To pursue these issues, the Ad Hoc Advisory Council on Cross-border Internet, which was commissioned by the Council of Europe, recommends the "multi-stakeholder participation" approach that is endorsed by the Council of Europe in such matters.

[292] Cf. Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP/PJA 2013, p. 837ff.

ment within the framework of existing regulations and to always ask whether a certain problematic development takes place exclusively in the field of social networks or whether it is transferable to other areas of life.

## 7.2 Review of a special law for social networks

### 7.2.1 Background

Postulat 11.3912 – "Rechtliche Basis für Social Media" [Postulate 11.3912 - "A Legal Basis for Social Media"] raised the question as to whether their development should be addressed by adopting a special legal regulation for social networks as is the case for radio and television.

### 7.2.2 Jurisdiction of the Confederation

It is important to first review whether the Confederation is the competent authority for the creation of provisions on social media content. The Confederation can rely on Art. 93 para. 1 of the Federal Constitution in relation to public communication on social media platforms. This constitutional provision declares that the Confederation is responsible for legislation on the dissemination of features and information by means of public telecommunications. The Confederation can make substantive regulations regarding these platforms, although in this case – in contrast to radio and television – performance mandates are not the direct result of the Constitution (Art. 93 para. 2 of the Federal Constitution). However the Confederation is free to specify, using the legislative process, content for other forms of dissemination of features and information by means of public telecommunications.[293] Based on this, the Confederation can fulfil its fundamental duty to protect the free, pluralistic exchange of information and ideas.

For content not addressed to the public which is exchanged via social networks, the Federal Council cannot rely on Art. 93 of the Federal Constitution. However, competencies in respect of regulation can be derived from various provisions in the Constitution. Thus Art. 92 para. 1 of the Federal Constitution describes telecommunications as a matter for the Confederation. On this basis, rules were promulgated in the Telecommunications Act not only concerning telecommunications transmissions but also, for example, on spamming or value-added services.[294] Moreover, the federal legislature can also rely for regulations under civil law on Art. 122 of the Federal Constitution and for regulations under criminal law on Art. 123. Within this framework, it would also be responsible for drawing up any special rules for social media, if necessary.

### 7.2.3 Need for special legal regulation?

A special regulation for public statements on social media comparable to that for broadcasting is only justified if it is necessary for the maintenance or promotion of free public communication. Given the diverse range of different social media platforms, this is to some extent less likely than in the area of radio and television, which has conventionally been characterised by a shortage of supply (frequency scarcity). The need for service mandates under multichannel conditions is also less pronounced than under monopoly conditions or at least in the case of one of the most clearly dominant (public) broadcasters on the market.

Regulation only appears necessary if free communication, as is required for the development of the individual and from a democratic point of view, cannot be guaranteed without appropriate action. This could for example be the case if the diversity that is essential for social and democratic processes is no longer reflected in the media, perhaps because minorities do not have any real chance to make their voices heard effectively.

---

[293] Official Bulletin 1983 no. 1353 (Votum Nationalrat Schüle) [Vote - National Councillor Schüle]

[294] Dispatch on the Amendment of the Telecommunications Act (TCA) of 12 November 2003, Federal Gazette 2003 7966, 8003.

However, within the field of social networks it cannot be ruled out that a few platforms could achieve a pre-eminence that is not adequately controlled by the free play of market forces. In this case, government intervention would be required to protect the diversity of opinion that is essential for social and democratic processes. This would, for example, be the case if certain population groups had no real opportunity to participate in communication via influential social media platforms. There is currently no indication of this; instead, it is assumed that minorities are also currently able to make themselves effectively heard on platforms. Apart from this, the majority of practically important providers are based abroad and the Swiss legislature's performance mandates would therefore be largely ineffective. There is currently no discernible need for special legal regulation in a specific social media law.

### 7.2.4 Need to amend existing legal standards?

As outlined, any response to the new problems created by social networks should not come about as the result of a special law or isolated individual regulations for social media, but through the adaptation of existing, often generically worded laws. Should this prove insufficient in individual cases, an amendment of existing legislation should be reviewed.

#### 7.2.4.1 In-depth review of data protection issues

Chapter 4 identified numerous data protection issues related to social media, among them the issue of the right to be forgotten and the general lack of control users have over their data.

The existing Swiss Data Protection Act is worded as a very generic framework. With prudent use the FADP allows the competent authorities and courts to also take into account new data protection issues. The question as to whether this applies without exception, or whether there may be a certain need for legal amendment, requires a more in-depth review, especially in terms of emerging revisions to data protection rules in the EU and the Council of Europe. The relevant investigative reviews are currently being undertaken under the auspices of the FDJP. A broad Data Protection Act (FADP) advisory group is analysing the entire data protection law and its enforcement measures. This includes the issues raised by new phenomena such as social media.

The FDJP's remit is to submit proposals for further action to the Federal Council by the end of 2014.

#### 7.2.4.2 Review to ascertain whether it is necessary to regulate the allocation of responsibility

As mentioned above (Section 5.3), given the current developments and the signals from the judiciary in relation to civil law it is advisable for the Federal Council to reconsider the need for legislative action to regulate the allocation of responsibility for internet service providers (including access and hosting providers). This review is challenging, especially as both in Switzerland and abroad a sophisticated legal practice has now developed; this should be analysed carefully. The relevant work is to be performed in 2013 under the auspices of the FDJP.

It cannot be ruled out that this work will include a review of other problem areas. These may include the question as to whether the current rules for the deletion or blocking of access to illegal content need to be adapted.

#### 7.2.4.3 Telecommunications law and social media platforms

Legal classification of the various transmission services that are sometimes also offered by social media platforms is difficult. Current telecommunications law, which was created at a time when there were no services that were separate from the underlying transport infrastructure, does not provide any suitable answers. Today, other business models are common (e.g. funding through advertising), technical conditions have changed and there is a much wider range of different transmission services, which can be offered all over the world with minimal expenditure. Which telecommunications law provisions should apply to which services is a question to be evaluated not only for social media, but for all services that can, for example, be provided (often for free) via the internet without having to ask one's own internet service provider for permission (so-called "over-the-top" services). These questions

will be addressed in greater depth in the consultation paper on the revision of the Telecommunications Act, a draft of which the Federal Council intends to submit during the current legislative period.

#### 7.2.4.4 Observation on whether data migration requires regulation

It is useful to follow the development of social media to see if operators attempt to keep their customers by preventing them from migrating their data to competitors (cf. 4.3.7 above). The Confederation should monitor this market and establish a right to data migration if the need arises. Regulating the interfaces between various social media platforms and for example making it mandatory for the largest to allow their users to exchange data and private messages with those of other platforms may also prove useful. It is possible that there will be empirical data from other countries about such laws in the coming years. This could also be used to assess the need for regulation.

## 7.3 Information and awareness raising

At both the international and national level, it is assumed that the opportunities and threats of social networks are influenced not only by legislation (and its enforcement). The best results can be achieved only by recourse to non-juridical instruments such as raising the awareness of those concerned.

### 7.3.1 Right to be forgotten

The European Network and Information Security Agency (ENISA) has pointed out that current technical solutions do not provide adequate protection for published data from unauthorised duplication by third parties and possible re-publication after the "official" deletion[295]. At the same time, it was established that on an open system such as the internet, purely technical solutions are insufficient for the implementation of the right to be forgotten; what is necessary is an interdisciplinary approach that defines the right to be forgotten both technically and legally[296].

However, being forgotten on social media platforms can in many cases be facilitated by anticipatory action. For example, the FDPIC recommends that prior to the publication of personal data users consider whether they would wish to be faced with that data in a future job interview – even in ten years' time[297]. It also recommends that no third-party personal data should be published. Although these principles are common knowledge, users should be repeatedly reminded of them and provided with illustrative examples. This could take place as part of the national "Jugend und Medien" [Young People and Media] programme, for example:

### 7.3.2 Infringement of personality rights, defamation, cyberbullying and cyberstalking

If social networks contain false assertions, defamatory value judgements or illegal exposure, criminal, civil and economic aspects of these are governed by Swiss law (see Section 4.4.1.3). Specific ways for private individuals to proceed if their personality rights are violated is described in Section 5.5.2. The problem remains that infringing content can spread so quickly and so far that it is unmanageable.

As far as cyberbullying and cyberstalking are concerned, the Federal Council has repeatedly stated that at present there is no indication that the existing criminal justice system would be insufficient (see Section 4.4.2.3).

However, the fact that the substantive legal status is clear in the case of infringement of personality rights, cyberbullying and cyberstalking, it cannot follow that this is also known to social media plat-

---

[295] European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten?searchterm=the+right+to+be+forgotten

[296] ENISA, The right to be forgotten, p. 11 ff.

[297] http://www.edoeb.admin.ch/datenschutz/00683/00690/00691/00693/index.html?lang=de#sprungmarke10_9 (only available in German, French and Italian).

forms users. An easily understandable introduction to the law, possibly supplemented by recommendations, might prove useful here. There are already vehicles for the school environment (such as the educa guides[298] or the "Jugend und Medien" [Young People and Media] platform[299]) that could be developed in this direction. In the case of other target groups and life contexts, there should be an examination into which channels and services are best suited to these tasks.

### 7.3.3 Children and young people

As mentioned above (Section 4.6.1.3), the Federal Council is to review measures to improve data protection for young people as part of the revision of the Data Protection Act.[300] Nevertheless, effective protection of young people from the media cannot be realised by legal instruments alone. The promotion of media literacy amongst children and young people as well as teachers and guardians in relation to the opportunities and threats of digital media is of central importance. This ties into the national "Jugend und Medien" [Young People and Media] programme[301], which was launched in a Federal Council Decision of 11 June 2010; it is to run from 2011-2015. The programme will help to ensure that parents, teachers and guardians have the necessary media skills to play an active role in monitoring the media activities of children and young people. For example, a reference portal for youth protection in Switzerland was established with www.jugendundmedien.ch (only available in German, French and Italian). The portal contains a schematic overview of the existing system, information and training opportunities in Switzerland as well as cantonal strategies and measures for protecting young people from the media. The "Medienkompetenz – Tipps zum sicheren Umgang mit digitalen Medien" [Media literacy - tips for dealing with digital media safely][302] brochure, which was published as part of the programme, provides parents, children and teachers with practical advice. It is devoted to subjects such as cyberbullying, instant messenger services, computer games, pornography and social networks, and explicitly addresses questions such as whether teachers and parents should be friends with young people on social networks. The programme also encourages cooperation between various agencies and stakeholders in the protection of young people from the media and supports professionals in awareness-raising activities. Quality assurance for existing services is promoted, as are innovative methods for teaching media literacy (peer education and access strategies for all sectors of the population).

Because the cantons are responsible for school education, their activities are of significance to the promotion of ICT skills. The Swiss Conference of Cantonal Ministers has a strategy for integrating ICT into schools[303]. Moreover, it has issued recommendations for training teachers in the field of information and communication technologies[304] as well as for the additional training profile for those working in the field of media education[305]. Teachers can find more on this subject at “educa.ch” (only available in German, French, and Italian). This education server offers teaching materials and further informa-

---

298 http://guides.educa.ch/de/recht (only available in German, French and Italian).

299 http://www.jugendundmedien.ch/home.html (only available in German, French and Italian).

300 Report concerning the evaluation of the Federal Act on Data Protection of 09 December 2011, no. 5.2.2 (BBl 2012 350).

301 http://www.jugendundmedien.ch/de.html (only available in German, French and Italian).

302 http://www.jugendundmedien.ch/fileadmin/user_upload/Chancen_und_Gefahren/Broschuere_FAQ_Medienkompetenz_dt.pdf (only available in German, French and Italian).

303 Strategie der EDK im Bereich Informations- und Kommunikationstechnologien und Medien [Swiss Conference of Cantonal Ministers of Education Strategy for Information and Communication Technology] of 01.03.2007 (http://edudoc.ch/record/30020/files/ICT_d.pdf?version=1) (only available in German). Also see the Erklärung zu den Informations- und Kommunikationstechnologien im Bildungswesen [Declaration on Information and Communication Technologies in the Education System] of 08.06.2000 (http://www.edudoc.ch/static/web/arbeiten/erkl_ikt_d.pdf).

304 Empfehlungen für die Grundausbildung und Weiterbildung der Lehrpersonen an der Volksschule und der Sekundarstufe II im Bereich der Informations- und Kommunikationstechnologien [Recommendation for Basic and Continuous Training of Primary, Secondary School I and Secondary School II Teaching Staff] of 25.04.2004; see: http://www.edudoc.ch/static/web/aktuell/medienmitt/empf_ict_lb_d.pdf (only available in German).

305 http://edudoc.ch/record/38148/files/Profil_ICT_d.pdf (only available in German).

tion including the "Safersurfing - Sicherheit in sozialen Netzwerken"[306], [Safer Surfing - Safety in Social Networks] information brochure by the Swiss Crime Prevention (SCP), which provides information on cyberbullying, sexual assault and the appropriate use of personal data. In January 2013, the SCP also published the "My little safebook" brochure for parents and young people on dealing with social media safely[307].

In addition to the aforementioned support measures, the Federal Council has commissioned the Federal Social Insurance Office (FSIO) to develop recommendations for the future structure of the protection of young people from the media in Switzerland as part of the national "Jugend und Medien" [Young People and Media] programme.

To achieve this task the FSIO has appointed a group of experts to assist it. The group comprises representatives of the Confederation, the cantons and industry, and has awarded four scientific mandates for developing sound principles:

Mandate 1 examines development and usage trends in digital media and the related challenges of protecting young people from the media (Autumn 2012 - Summer 2013)

Mandate 2 conducts a survey and review of the regulatory activities of the cantons (Spring 2013 - Summer 2014).

Mandate 3 evaluates the implementation and impact of self-regulatory measures by the film, computer game, telecommunications, and internet industries in Switzerland (Spring 2013 - Summer 2014).

Mandate 4 analyses media-specific and cross-media regulatory models in different countries, identifies "good practice" examples and formulates recommendations for Switzerland (Spring 2013 - Summer 2014).

The aim is to determine by 2015 the need for regulation on a federal level and whether the creation of constitutional principles is necessary.

### 7.3.4 Improving the media literacy of the population

As stated above, within the school environment there is already a considerable amount being done to improve the media skills of children and young people, as well as those who care for them. As social media is a very young and therefore dynamic phenomenon, relevant websites, publications etc. must be continually reviewed for their relevance and if necessary revised.

In addition, it is necessary to review the extent to which improving media literacy is required in other target groups, particularly in relation to the use of social media.[308] Furthermore, increased use of social media itself makes sense for all target groups in order to provide information and raise awareness on selected issues.

---

[306] http://guides.educa.ch/sites/default/files/sicherheit_netzwerke_d.pdf (only available in German).

[307] http://news.skppsc.ch/de/2013/01/24/neue-broschure-my-little-safebook-fur-einen-sicheren-umgang-mit-den-sozialen-medien/ (only available in German).

[308] Campaigns such as the cartoon brochure "Stories from the internet that no-one wants to experience" target a wide audience, see http://www.geschichtenausdeminternet.ch/index_en.html.

# 8 Response to questions in the postulate

The questions raised in the postulate can be answered as follows in accordance with the statements above:

- What is the current legal status in Switzerland and internationally in terms of social media?

Current legislation both in Switzerland and other countries is characterised by the fact that as far as can be discerned virtually no regulations have been created that specifically and exclusively relate to the new phenomenon of social media. Instead, the existing legal standards have to date been applied to communication on social networks.

- How does the Federal Council view the creation of a specific social media law that takes into account the specific characteristics of these new forms of communication?

There is currently no discernible need for a specific social media law modelled on the previous special legal regulation of radio and television.

- Where there are gaps in the law and how they can be closed?

Experience to date has shown no major gaps in existing Swiss law. With careful application, the provisions of existing laws (e.g. the FADP, SCC, CC and UCA), which are often worded generically, allow a reasonable response to most problems that social platforms do or might create for individuals and the general public. However, whether these rules will work in practice is uncertain. Specific improvements appear possible in some areas. For this reason, investigations in various respects (e.g. in terms of data protection and the protection of young people) are necessary or already underway. It should be kept in mind that the relevant investigations are not limited to social media, but also touch on a variety of other issues.

# 9 Further action

As shown in Chapter 7, there are currently several substantial activities underway within the Federal Administration that also address a possible legal regulation of social media.

Data protection issues are being discussed in the context of the ongoing revision work on the FADP (under the auspices of the FDJP). The issues raised by social platforms are just one of many subjects to be examined as part of this work. The results are of key importance to the legal issues surrounding the lack of control users have over their data on social networks (and certain improvements through, for example, privacy-friendly default settings), and the right to be forgotten. The FDJP's remit is to submit proposals for further action to the Federal Council by the end of 2014.

Issues relating to protecting young people from the media will be analysed by 2015 as part of the "Jugend und Medien" [Young People and Media] programme, which is supervised by the Federal Office for Social Insurance. As part of this, it will be determined whether there is a need for regulation at a federal level and whether a new legal basis is necessary to protect children and young people from the media in Switzerland. Recommendations for the future structure of the protection of young people from the media in Switzerland will also be developed.

It is necessary to examine whether legislative action is necessary with regard to civil law in order to regulate the allocation of responsibility of platform operators and technical service providers (access and hosting providers). These investigations are not confined to the phenomenon of social networks; instead they relate to the legal responsibility of online service providers in general. The EJPD will address this issue and, in the event that the need to amend the law is approved, submit a consultation paper to the Federal Council.

Issues relating to telecommunications law will be addressed as part of the consultation paper on the revision of the TCA. According to current planning this will be commissioned by the Federal Council during the current legislative period.

The question of whether social media platforms will attempt to retain their customers by preventing them from migrating their data to competitors does not yet require regulation, but should be monitored with regard to possible regulation. It may in future prove necessary to introduce a right to data migration or to regulate the interfaces between social media platforms. Any regulatory activities in other countries should also be monitored.

As previously mentioned, the various activities and investigations concern not only social media, but are to be considered in the context of the legal system as a whole. However, it is important that the various aspects including social media be combined to create a coherent overall picture. For this reason, it is essential that the flow of information between the government offices involved is ensured.

Given the large number of known – but also any other – regulatory activities that are of more or less considerable relevance to social media, the risk of losing sight of the overall problem cannot be denied. In the medium term it therefore appears appropriate to carry out a review from the perspective of social media at the appropriate time. This analysis will incorporate the rapid development on the international level and the emerging jurisprudence on many issues. There is a good chance of deriving information regarding the strengths and weaknesses of the existing regulations from this.

Overall, a review of the current position concerning the legal basis for social media would seem advisable by the end of 2016, when the aforementioned work is complete and the direction it is going in is clearly visible; this would act as an interim report.

# 10 Abbreviations, bibliography and sources

## 10.1 Glossary of abbreviations

| | |
|---|---|
| AGUR12 | Working group on the optimisation of the collective management of copyright and related rights |
| BGBl | Bundesgesetzblatt [Official public bulletin of the Federal Republic of Germany] |
| Blog | Web log, a journal or diary on a website |
| CartA | Cartels Act |
| CC | Swiss Classified Compilation of Federal Law |
| cf. | compare |
| CO | Code of Obligations |
| CYCO | Cybercrime Coordination Unit Switzerland |
| DDA | Elimination of Discrimination against People with Disabilities Act |
| DDO | Elimination of Discrimination against People with Disabilities Ordinance |
| e.g. | for example |
| ECHR | European Convention on Human Rights |
| ECJ | European Court of Justice (the European Union's highest judicial body) |
| ECtHR | European Court of Human Rights |
| Ed. | Editor |
| EDK | Swiss Conference of Cantonal Ministers of Education |
| EESC | European Economic and Social Committee |
| ENISA | European Network and Information Security Agency |
| EU | European Union |
| FADP | Data Protection Act |
| FC | Federal Constitution |
| FDJP | Federal Department of Justice and Police |
| FDPIC | Federal Data Protection and Information Commissioner |
| fn. | Footnote |
| FoodO | Ordinance on Foodstuffs |
| FOPH | Federal Office of Public Health |
| FTC | Federal Trade Commission (federal competition and consumer rights authority for the USA) |
| H.R. | House of Representatives (of the US Congress) |
| ICT | Information and communication technologies |
| IPRG | International Private Law Act |
| JCLA | Juvenile Criminal Law Act |
| JCrimPC | Juvenile Criminal Procedure Code |
| KJFG | Children and Young People Act |
| KJFV | Children and Young People Ordinance |
| MCC | Military Criminal Code |
| no. | Number |
| OFCOM | Federal Office of Communications |
| OJEC | Official Journal of the European Union |
| P2P | Peer-to-peer |

| | |
|---|---|
| RSS | Really Simple Syndication, format for the structured publication of amendments to websites |
| RTVA | Radio and Television Act |
| RTVO | Radio and Television Ordinance |
| SCP | Swiss Crime Prevention |
| SECO | State Secretariat for Economic Affairs |
| simsa | Swiss Internet Industry Association |
| SRG | Swiss Broadcasting Corporation (SRG SSR) |
| TCA | Telecommunications Act |
| TPA | Medicinal Products Act |
| TPAO | Ordinance on the Advertising of Therapeutic Products |
| U.S.C. | United States Code (collection and codification of US federal law) |
| WLAN | Wireless Local Area Network |

## 10.2 Bibliography


Aguiton C./Cardon D., The Strength of Weak Cooperation: an Attempt to Understand the Meaning of Web 2.0, Communication & Strategies, no. 65, 1st quarter 2007 (**cited as Aguiton C./Cardon D.**)

Bächli Marc, Das Recht am eigenen Bild. Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus der Sicht der abgebildeten Person, Basel 2002 (**cited as Bächli Marc, Das Recht am eigenen Bild, Basel 2002**)

Baeriswyl Bruno, Kleingedrucktes unter der Lupe - Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, in: digma 2010 p. 56

Bianchi della Porta Manuel/Robert Vincent, Responsabilité pénale de l'éditeur de médias en ligne participatifs, in: medialex 2009, p. 19ff.

Boyd D.M./Ellison N.B., Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), article 11, 2007 (**cited as Boyd D.M./Ellison N.B.**)

Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, in: Jusletter, 17.01.2011

Elixmann Robert, Datenschutz und Suchmaschinen. Neue Impulse für den Datenschutz im Internet, Berlin 2012

Engel C./Knieps G., Vorschriften des Telekommunikationsgesetzes über den Zugang zu wesentlichen Leistungen: Eine juristisch-ökonomische Untersuchung, Baden-Baden 1998. (**cited as Engel C./Kniwps G.**)

Epiney Astrid/Fasnacht Tobias (eds.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes, Zurich 2012

European Network and Information Security Agency (ENISA), The right to be forgotten – between expectations and practice, Heraklion 2011

Epiney Astrid/Probst Thomas/Gammenthaler Nina (eds.), Datenverknüpfung. Problematik und rechtlicher Rahmen, Zurich 2011

Hilty Lorenz/Oertel Britta/Wölk Michaela/Pärli Kurt, Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern, Zurich 2012 (**cited as Hilty/Oertel/Wölk/Pärli, Lokalisiert und identifiziert, Zurich 2012**)

Jöhri Yvonne, Werbung im Internet: rechtsvergleichende, lauterkeitsrechtliche Beurteilung von Werbeformen, Zurich 2000 (**cited as Jöhri Yvonne, Werbung im Internet, Zurich 2000**)

Keller Claudia, AGB von Social-Media-Plattformen, in: medialex 2012 p. 188ff.

Latzer M./Just N./Metreveli S./Saurwein F. (2012). Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project – Switzerland 2011. University of Zurich, Zurich

Mayer-Schönberger Viktor, Delete: Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010

Meyer Julia, Identität und virtuelle Identität natürlicher Personen im Internet, Baden-Baden 2011

Neuberger, Christoph, "Soziale Netzwerke im Internet. Kommunikationswissenschaftliche Einordnung und Forschungsüberblick". in: Neuberger, Christoph; Gehrau, Volker (eds.): StudiVZ. Diffusion, Nutzung und Wirkung eines sozialen Netzwerks im Internet. Wiesbaden 2011, p. 33 - 96

Schmidt, Jan, "Was ist neu am Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen". in: Zerfass, Ansgar; Welker, Martin; Schmidt, Jan (eds.): Kommunikation, Partizipation und Wirkungen im Social Web. Vol. 1, Cologne 2008, p. 18 - 40

Schweizer Alex, Data Mining – ein rechtliches Minenfeld. Rechtliche Aspekte von Methoden des Customer Relationship Management (CRM) wie Data Mining, in: digma 2001 p. 108

Schweizer Michael, Das Recht am Wort nach Art. 28 ZGB, in: medialex 2011 p. 197ff.

Schweizer Michael, Recht am Wort: Schutz des eigenen Wortes im System von Art. 28 ZGB, Bern 2012 (**cited as Schweizer Michael, Recht am Wort, Bern 2012**)

Streiff Ullin/von Kaenel Adrian/Roger Rudolph, Arbeitsvertrag Praxiskommentar, 7th ed., Zurich 2012

Studer Melanie/Schweizer Matthias/Brucker-Kley Elke, Sterben und Erben in der digitalen Welt, in: Jusletter 17.12.2012

Von Rimscha M. Björn, Geschäftsmodelle für Social Media . In: Petra Grimm und Oliver Zöllner (ed.): Schöne neue Kommunikationswelt oder Ende der Privatheit? Die Veröffentlichung des Privaten in Social Media und populären Medienformaten. Stuttgart 2012, p. 297 – 311

Weber Rolf, E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2nd ed., Zurich 2010

Weber Rolf/Volz Stephanie, Online Marketing und Wettbewerbsrecht, Zurich 2011

## 10.3 Glossary of laws

Federal Act of 15 December 2000 on Medicinal Products and Medical Devices (TPA), CC 812.21

Federal Act of 13 December 2002 on the Elimination of Discrimination against People with Disabilities (DDA), CC 151.3

Federal Act of 19 June 1992 on Data Protection (FADP), CC 235.1

Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations), CC 220

Bundesgesetz vom 30. September 2011 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFG) [Federal Act of 30 September on Promoting Extra-Curricular Work with Children and Young People], CC 446.1

Federal Act of 18 December 1987 on International Private Law (IPRG), CC 291

Federal Act of 20 June 2003 on the Criminal Law applicable to Juveniles (JCLA), CC 311.1

Federal Act of 6 October 1995 on Cartels and other Restraints of Competition (CartA), CC 251

Federal Act of 24 March 2006 / 29 May 2013 on Radio and Television (RTVA), CC 784.40

Federal Act of 19 December 1986 on Unfair Competition (UCA), CC 241

Federal Act of 9 October 1992 on Copyright and Neighbouring Rights (CopA), CC 231.1

Federal Constitution of the Swiss Confederation of 18 April 1999, CC 101

Telecommunications Act of 30 April 1997 (TCA), CC 784.10

European Convention of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms (ECHR), CC 0.101

Military Criminal Code of 13 June 1927 (MCC), CC 321.0

Swiss Juvenile Criminal Procedure Code of 20 March 2009 (JCrimPC), CC 312.1

Swiss Criminal Code of 21 December 1937 (SCC), CC 311.0

Swiss Civil Code of 10 December 1907 (SCC), CC 210

Convention of 23 November 2001 on Cybercrime (CCC), CC 0.311.43

Convention of 30 October 2007 on Jurisdiction and the Recognition and Enforcement of Judgements in Civil and Commercial Matters (new LugC), CC 0.275.12

Convention of 20 November 1989 on the Rights of the Child, CC 0.107

Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten [Convention of 28 January 1981 on the Protection of Individuals in the Case of Automatic Processing of Personal Data], CC 0.235.1

Übereinkommen Nr. 182 vom 17. Juni 1999 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit [Convention no. 182 of 17 June 1999 on the Prohibition of and Immediate Measures to Eliminate the Worst Forms of Child Labour], CC 0.822.728.2

FDHA Ordinance of 23 November 2005 on Alcoholic Beverages, CC 817.022.110

Ordinance 5 of 28 September 2007 to the Employment Act - Youth Employment Protection Ordinance (EmpO 5), CC 822.115

Ordinance of 17 October 2001 on the Advertising of Therapeutic Products (TPAO), CC 812.212.5

Verordnung des WBF vom 4. Dezember 2007 über gefährliche Arbeiten für Jugendliche [Ordinance of the EAER of 4 December 2007 on Hazardous Work for Young People], CC 822.115.2

Ordinance of 19 November 2003 on the Elimination of Discrimination against People with Disabilities (EPDO), CC 151.31

Verordnung vom 17. Oktober 2012 über die Förderung der ausserschulischen Arbeit mit Kindern und Jugendlichen (KJFV) [Ordinance of 17 October 2012 on Promoting Extra-Curricular Work with Children and Young People], CC 446.11

Ordinance of 23 November 2005 on Foodstuffs and Utility Articles (FoodO), CC 817.02

Radio and Television Ordinance of 9 March 2007 (RTVO), CC 784.401

Verordnung vom 11. Juni 2010 über Massnahmen zum Schutz von Kindern und Jugendlichen sowie zur Stärkung der Kinderrechte [Ordinance of 11 June 2010 on Measures to Protect Children and Young People and to Improve Children's Rights], CC 311.039.1

Ordinance of 1 March 1995 on Tobacco and Tobacco Products (TobO), CC 817.06

## 10.4 Glossary of abbreviated international material

### 10.4.1 Council of Europe

Abridged Report of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no. 108) - 29th Plenary Meeting of 10 December 2012, T-PD (2012) RAP 29 Abr_en (**cited as Abridged Report of the Consultative Committee of Convention 108, T-PD (2012) RAP 29 Abr_en**)

Ad Hoc Advisory Group on Cross-Border Internet, 4th meeting, executive summary of 13 & 14.10.2011 (**cited as Ad Hoc Advisory Group on Cross-Border Internet**)

Recommendation Rec(2004)16 of the Committee of Ministers of the Council of Europe of 15.12.2004 on the Right of Reply in the New Media Environment (**cited as Recommendation Rec(2004)16 on the Right of Reply in the New Media Environment**)

Recommendation Rec(2006)12 of the Committee of Ministers of the Council of Europe of 27.09.2006 on empowering children in the new information and communications environment (**cited as Recommendation Rec(2006)12 on empowering children in the new information and communications environment**)

Recommendation CM/Rec(2007)2 of the Committee of Ministers of the Council of Europe of 31.01.2007 on media pluralism and diversity of media content (**cited as Recommendation CM/Rec(2007)2 on media pluralism and diversity of media content**)

Recommendation CM/Rec(2008)6 of the Committee of Ministers of the Council of Europe of 26.03.2008 on measures to promote the respect for freedom of expression and information with regard to internet filters (**cited as Recommendation CM/Rec(2008)6 on measures to promote the respect for freedom of expression and information with regard to internet filters**)

Recommendation CM/Rec(2009)5 of the Committee of Ministers of the Council of Europe of 08.07.2009 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment **(cited as Recommendation CM/Rec(2009)5 on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment)**

Recommendation CM/Rec(2010)13 of the Committee of Ministers of the Council of Europe of 23.11.2010 on the protection of individuals with regard to automatic processing of personal data in the

context of profiling (**cited as Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling**)

Recommendation CM/Rec(2011)7 of the Committee of Ministers of the Council of Europe of 21.09.2011 on a new notion of media (**cited as Recommendation CM/Rec(2011)7 on a new notion of media**)

Recommendation CM/Rec(2011)8 of the Committee of Ministers of the Council of Europe of 21.09.2011 on the protection and promotion of the universality, integrity and openness of the Internet (**cited as Recommendation CM/Rec(2011)8 on the protection and promotion of the universality, integrity and openness of the Internet**)

Recommendation CM/Rec(2012)3 of the Committee of Ministers of the Council of Europe of 04.04.2012 on the protection of human rights with regard to search engines (**cited as Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines**)

Recommendation CM/Rec(2012)4 of the Committee of Ministers of the Council of Europe of 04.04.2012 on the protection of human rights with regard to social networking services (**cited as Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services**)

Declaration of the Committee of Ministers of the Council of Europe of 07.12.2011 on the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers (**cited as the Declaration on the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers**)

Declaration of the Committee of Ministers of the Council of Europe of 21.09.2011 on internet governance principles (**cited as the Recommendation on internet governance principles**)

Declaration of the Committee of Ministers of the Council of Europe of 20.02.2008 on protecting the dignity, security and privacy of children using the internet (**cited as the Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children using the internet**)

Modernisation of Convention 108: New Proposals of The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS no. 108) of 27.04.2012, T-PD-BUR(2012)01Rev2_en (**cited as Modernisation of Convention 108, T-PD-BUR(2012)01Rev2_en**)

### 10.4.2 European Union

Opinion of the Article 29 Working Party 02/2012 on facial recognition in online and mobile services 22.03.2012, 00727/12/DE WP 192 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2 (**cited as Art. 29 Working Party Opinion 00727/12/DE WP 192**)

Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 13.09.2011 on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity and of the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and online information services industry – Protecting Children in the Digital World –, COM(2011) 556 final (**cited as Report from the Commission, COM(2011) 556 final**)

Decision 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other com-

munication technologies, OJEC L 348 of 24.12.2008 (**cited as Decision 1351/2008/EC establishing a multiannual Community programme on protecting children using the Internet and other communication technologies**)

Recommendation of the European Parliament of 26.03.2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)), OJEC C 117 E of 06.05.2010 (**cited as the recommendation of the EU Parliament on strengthening security and fundamental freedoms on the Internet, (2008/2160(INI))**)

Recommendation of the European Parliament and of the Council of 20.12.2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, 2006/952/EG, OJEC L 378 of 27.12.2006 (**cited as the recommendation on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, 2006/952/EG**)

Resolution of the European Parliament 15.12.2010 on the impact of advertising on consumer behaviour (2010/2052(INI)), OJEC C 169 E of 15.06.2012 (**cited as resolution on the impact of advertising on consumer behaviour (2010/2052(INI)**

Joint Communication to the European Parliament and the Council "Human rights and democracy at the heart of the EU external action – Towards a more effective approach" of 12.12.2011, COM(2011) 886 final (**cited as Joint Communication "Human rights and democracy at the heart of the EU external action", COM(2011) 886 final**)

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Europe's Digital Competitiveness Report: Main achievements of the i2010 strategy 2005-2009" of 04.08.2009, COM(2009) 390 final (**cited as Communication "Europe's Digital Competitiveness Report: Main achievements of the i2010 strategy 2005-2009", COM(2009) 390 final**)

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "European Strategy for a Better Internet for Children" of 02.05.2012, COM(2012) 196 final (**cited as Communication "European Strategy for a Better Internet for Children", COM(2012) 196 final**)

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Interim evaluation of the multi-annual Union programme on protecting children using the Internet and other communication technologies" of 03.02.2012, COM(2012) 33 final (**cited as Communication from the Commission "Interim evaluation of the multi-annual Union programme on protecting children using the Internet and other communication technologies", COM(2012) 33 final**)

Communication from the Commission to the Council and the European Parliament on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre of 28.03.2012, COM(2012) 140 final (**cited as the Communication on Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final**)

Directive 2011/83/EU of the European Parliament and of the Council of 25.10.2011 on consumer rights, amending Directive 93/13/EEC and Directive 1999/44/EC repealing Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJEC. L 304 of 22.11.2011 (**cited as Directive 2011/83/EU of 25.10.2011 on consumer rights, amending Directive 93/13/EEC and Directive 1999/44/EC repealing Directive 85/577/EEC and Directive 97/7/EC**)

Directive 95/46/EG of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

OJEC L 281 of 23.11.1995 (**cited as Directive 95/46/EG on the protection of individuals with regard to the processing of personal data and on the free movement of such data**)

Conclusion of the Council of 11.05.2012 on fostering the creative and innovative potential of young people, OJEC C 169 of 15.06.2012] (**cited as the Conclusion on fostering the creative and innovative potential of young people, 2012/C 169/01**)

Opinion of the European Economic and Social Committee on "The Internet of Things" of 18.09.2008, OJEC C 077 of 31.03.2009 (**cited as the Opinion on "The Internet of Things" 2009/C 77/15**)

Opinion of the Committee of the Regions on "The digital agenda for Europe", OJEC C 015 of 18.01.2011 (**cited as Opinion of the Committee of the Regions on "The digital agenda for Europe'", 2011/C 15/07**)

Opinion of the European Economic and Social Committee on the "Responsible use of social networks and the prevention of related problems" of 19.09.2012, OJEC C 351 of 15.11.2012 (**cited as Opinion of the European Economic and Social Committee on the "Responsible use of social networks and the prevention of related problems", 2012/C 351/07**)

Proposal of a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 25.01.2012, COM(2012) 11 final (**cited as EU Proposal General Data Protection Regulation, COM(2012) 11 final**)

### 10.4.3 Germany

Antwort der Bundesregierung auf die kleine Anfrage "Rechtsextremismus im Internet" vom 07.06.2010, Drucksache 17/1930 [Reply from the Federal Government to the brief enquiry "Right-Wing Extremism on the Internet" of 07.06.2010, printed matter 17/1930] (**cited as Antwort der Bundesregierung auf die kleine Anfrage "Rechtsextremismus im Internet", 17/1930**)

Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes vom 03.08. 2011, Drucksache 17/6765 [Draft amendment of the Bundesrat to the Telemedia Act of 03.08. 2011, printed matter 17/6765] (**cited as Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes, 17/6765**)

Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes vom 15.12.2010, Drucksache 17/4230 [Draft legislation of the Bundesrat to regulate the Workplace Privacy Act of 15.12.2010, printed matter 17/4230 (**cited as Gesetzesentwurf Beschäftigtendatenschutz, 17/4230**)

## 10.5 Studies and reports

Bernet ZHAW Studie Social Media Schweiz 2012

eHealth Suisse Bericht Öffentliches Gesundheitsportal

ENISA Threat Landscape Report of 28.09.2012

EU Kids Online Final Report, September 2011

2011 and 2012 Annual Reports by the Cybercrime Coordination Unit Switzerland (CYCO)

Optimus study "Sexuelle Übergriffe an Kindern und Jugendlichen in der Schweiz", February 2012

Stiftung Warentest "Datenschutz bei Onlinenetzwerken", 2010

Federal Statistical Office's study on "Internet in den Schweizer Haushalten. Ergebnisse der Erhebung Omnibus IKT 2010"

Unpublished figures from the netTEEN-Studie (Perren S. & Sticca F., 2012. Jacobs Center for Productive Youth Development, University of Zurich)

Wikimedia Foundation: Annual Report 2010/2011