Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 679-693

This document is part of the Comparative Study on blocking, filtering and take-down of illegal internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member states, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?

- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

SWITZERLAND

1. Legal Sources

Apart from two provisions in isolation (one in the Federal Law on Internal Security and the other in the Ordinance on Internet Domains),[1] **Switzerland has no particular rules on blocking, filtering and removing Internet content**. In practice, both parliament and the government rely on ordinary law to address this new issue; accordingly, they leave it to the courts to make the necessary adjustments, where appropriate. This lack of specific rules is not surprising; it reflects the confusion felt by the legislature unable to keep pace with a complex communication process, phenomenal technical progress and uncontrollable globalisation. One example among others is the recent statement by the Swiss government (the Federal Council) in its report on the absence of any need to regulate social networks: "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".[2]

However, this hands-off approach by the legislature has created **considerable uncertainty with regard to the legal framework governing online communication**. There are two reasons for this: first, as we shall see, ordinary law is not always able to regulate a means of communication which is very different from conventional communication; certain Internet procedures require special solutions. Second, the courts interpret the law only on the basis of the cases submitted to them. In other words, the case-law in this area is still somewhat ad hoc and fragmentary: the Federal Court, the highest Swiss court, has only very occasionally had to deal with the legal aspects of online communication and there are many fundamental issues which remain unresolved, first of which is the level of diligence of service providers and the extent of their liability.

A further reason why this question, lying at the very heart of this legal opinion, has not been specifically addressed by the legislature, is that Switzerland is not a member of the European Economic Area, and even less so of the European Union. Accordingly, it has not been obliged to implement the Community texts on this issue, namely Directive 2000/31 EC on electronic commerce and Directive 2002/58 EC on privacy and electronic communications. Nor is Switzerland concerned by the case-law in this area of the Court of Justice of the European Union (beginning with the L'Oréal,[3] Google France[4] and Scarlet Extended[5] judgments).

In the matter of interest to us here, it is primarily ordinary law, technically neutral (and therefore supposedly able to cope with any developments in communication mediums), which will, with varying degrees of facility, be applied. These general rules, listed in summary form below, will be discussed in greater detail in the following sections.

- Measures to prevent or halt violations, provided for in the rules on the protection of personality rights laid down in the Civil Code, the Copyright Act, the Unfair Competition Act and the Data Protection Act.[6]

---

1 These provisions will be discussed in greater detail below, cf. 2.1.5 and 2.1.6.

2 Legal Basis for Social Media: Report of the Federal Council in fulfilment of the Amherd postulate 11.3912 of 29 September 2011, Bern 2013, p. 70.

3 Judgment of 12 July 2011, L'Oréal SA and others v. eBay International AG (C-324/09).

4 Judgment of 23 March 2010, Google France SARL and Google Inc. v. Louis Vuitton Malletier SA (C-236/08 to C-238/08).

5 Judgment of 24 November 2011, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (C-70/10).

6 See below 2.1.1 to 2.1.4.

- The various possibilities for seizure or forfeiture provided for in criminal law (Criminal Code or Criminal Procedure Code).[7]
- The administrative measures to protect public order or implement special laws (the Gaming Act, the Alcohol Act, the Therapeutic Products Act, the Internal Security Act, etc.).[8]

While the legal framework governing online communications in Switzerland may be described as rudimentary and contingency-based, it should nonetheless be noted that, here and there, a number of specific rules have been adopted in response to urgent concerns (such as spamming, electronic signatures, e-voting or online casinos) or to implement international conventions, directly or indirectly relating to the Internet, ratified by Switzerland. To date there are five such conventions:

- The two treaties of the World Intellectual Property Organisation of 20 December 1996 on copyright and on performances and phonograms.[9]
- The Council of Europe Convention on Cybercrime (ETS 185) of 23 November 2001[10] containing substantive and procedural law measures to combat the increase in online crime.[11]
- The Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) of 28 January 1981.[12]
- The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) of 25 October 2007.[13]

It will be noted that two major Council of Europe texts have not yet been ratified by Switzerland: the Protocol on Xenophobia and Racism committed through computer systems (ETS 189)[14] and the Convention on the Prevention of Terrorism (CETS 196).[15]

Lastly, it should be noted that a number of authors and an increasing number of politicians and business representatives are calling on the legislature to take a more proactive approach in order to at long last bring about the legal security that is needed.[16] So far without success: after having proceeded with an in-depth analysis of the situation by internal experts at the Federal administration, the the Swiss Government clarified at the end of 2015 that the status quo should be maintained. According to the Government, even if there is a lack of clarity, there is no need to

---

7 See below 2.1.5.

8 See below 2.1.6.

9 Respectively the Systematic Compendium of Federal Legislation (hereafter RS) 0.231.151 and 0.231.171.1. These were transposed into Swiss law by means of a recent revision of the Federal Copyright Act (Official Compendium of Federal Acts (hereafter RO) 2008 2497).

10 RS 0.311.43.

11 For an analysis of the impact of this convention on Swiss law see the Federal Council Statement on the ratification of the Cybercrime Convention, Federal Law Gazette (hereafter FF) 2010 475 et seq.; see also Cassani U., "Chronique de droit pénal suisse dans le domaine international (2010)", in *Revue Suisse de droit international et européen* 2011, p. 515 et seq.

12 RS 0.235.1. This text was supplemented by the Additional Protocol of 8 November 2001 regarding supervisory authorities and transborder data flows, also ratified by Switzerland (RS 0.235.11).

13 RS 311.040.

14 This was criticised by the European Commission against Racism and Intolerance (ECRI), which strongly urged Switzerland to ratify this additional Protocol as soon as possible (report on Switzerland 2009, p. 11, paragraph 7). So far, in vain.

15 It is probable that Switzerland will ratify this convention in the near future; a motion to this effect is currently being discussed in parliament (Motion 14.4187).

16 For further details, see Cottier B., "Le droit 'suisse' du cyberespace ou le retour en force de l'insécurité juridique et de l'illégitimité", *Revue de droit suisse* 2015 II, p.226 et seq.

legislate with regard to the liability of Internet Service Providers (ISPs),[17] except in order to establish specific rules on blocking and take-down in the areas of copyright and online gaming.[18]

2. Applicable regulations

2.1. Blocking and/or filtering of unlawful website content

2.1.1. Protection of personality rights

Under Article 28, paragraph 1 of the Civil Code (hereafter CC), "Any person whose personality rights are unlawfully infringed may petition the court for protection against all those causing the infringement." In practice, this provision enables victims of an infringement of their personality rights (in particular defamation or violation of privacy) to apply to the civil courts to have that infringement ceased. Similarly, victims may, where applicable, ask the court to prevent a future infringement, provided that it is imminent and serious.[19] In the interests of greater effectiveness, the court order in most cases is accompanied by the threat of criminal penalties in the event of failure to comply.[20]

Unlike remedial action for damages – which can only be taken against a person guilty of malicious intent or gross negligence – **an action to protect personality rights established by Article 28.1 CC may be taken against any person who contributes, directly or indirectly, to the commission of the infringement**. As underlined by the established case-law of the Federal Court "among the legitimate defendants in such actions is anyone who "contributes" to the infringement. This covers not only the original perpetrator of the infringement but anyone whose collaboration causes, enables or encourages the said infringement, without the need for any tortious intent on his or her part (…). The mere fact of collaboration constitutes (objectively) an infringement, even if the person in question is not or cannot even be aware of the fact (…). In other terms, this can be anyone who, without being the author of the remarks complained of or even being aware of their substance or knowing their author, contributes to their dissemination. The injured party may take action against anyone who has objectively played a role, directly or indirectly – even if only secondary – in the bringing about or furthering of the infringement".[21] On the basis of this broad interpretation of the concept of "contributing to the infringement", the Federal Supreme Court acknowledged that in the traditional press field, court action can be taken against not only the author of an article infringing personality rights under Article 28.1 CC, but also the publisher, printer or even a newsagent selling the newspaper in question.[22]

It should also be pointed out that **Art. 28 CC lays down no order of priority; it is for the injured party to decide freely against whom he or she wishes to initiate proceedings**.[23]

---

17 Report of the Federal Council of 11 December 2015, Bern 2015, p. 97ss.

18 See, respectively the end of sections 2.1.3. and 2.2.2. of this country report, as well as 2.1.6.

19 Federal Supreme Court judgment 128 III 100.

20 In application of Article 292 of the Criminal Code which provides that anyone who fails to comply with an official order shall be liable to a fine.

21 Federal Supreme Court judgment of 14 January 2014 (recital. 6), 5A_792/2011; likewise, the judgment of 6 May 2015, 5A_658/2014 (recital 4.2). See also the Federal Council Statement of 5 May 1982 concerning the revision of the Swiss Civil Code [Protection of personality rights: Article 28 CC and Article 49 Code of Obligations (CO)], FF 1982 II 681.

22 Federal Supreme Court judgment 131 III 26.

23 "The principle of proportionality, which must be respected in the actions provided for in Article 28a CC and in the provisional measures provided for in Article 28c CC (…), does not preclude a measure being issued against a single protagonist, even where the latter is secondary, against whom the applicant has

To date, the Federal Supreme Court has not yet had occasion to hear cases involving Internet Service Providers (hereafter ISPs). As to legal doctrine, this is divided. Certain legal authors are of the opinion that ISPs could be obliged to block the IP address of sites containing online data infringing personality rights, as even though they did not originate the infringing communications, they contribute to their dissemination on the worldwide web. However, such blocking must target only the infringing content and not prevent access to other communications which are lawful (prohibition of overblocking).[24] Other authors, on the other hand, doubt that it would be possible to successfully sue ISPs, on account of a lack of sufficient causation between their involvement and the resulting harm.[25]

2.1.2. Data protection

The Federal Data Protection Act (hereafter DPA[26]), which implements Council of Europe Convention 108 referred to above (see Section 1), also provides for legal remedies to prevent unlawful processing of personal data. Insofar as the disputed treatment is carried out by a natural or legal person under private law,[27] these remedies are identical to those that may be relied on in order to protect personality rights; Article 15 DPA explicitly refers to the actions provided for in Article 28 CC discussed above (see 2.1.1).[28]

Consequently, ISPs may be forced by the civil courts to block access to information derived from the unlawful processing of data, even if they themselves have not committed any fault.

2.1.3. Intellectual property

Both the Federal Copyright Act (hereafter (FCA[29]) and the Federal Act on the Protection of Trade Marks and Indications of Source (*Trade Mark Protection Act*, hereafter the TMPA[30]) provide for the possibility of applying to the court to halt (or where appropriate prevent) a violation of copyright or law or trade mark law (see Article 62.1 FCA and Article 55 TMPA). These actions are similar in all respects to the actions to protect personality rights provided for in the Civil Code (see 2.1.1 above). In particular the range of persons who can be cited as defendants is equally broad, even though, unlike Article 28 CC the wording of the two provisions makes no explicit reference to the fact that action can be brought against any natural or legal person who has "contributed" to the violation.[31]

---

decided to take action", Federal Supreme Court judgment of 12 September 2002 (5P.254/2002), recital 2.5.

24 Rosenthal David, "Internet-Provider-Haftung – ein Sonderfall?" in: Jung P. (Ed.), *Aktuelle Entwicklungen im Haftungsrecht*, Bern/Zürich/Basel/Geneva, 2007, p. 158.

25 The Swiss Government concurred with this point of view in its report of December 2015 (see footnote 17), p.32.

26 RS 235.1.

27 The judicial remedies against processing carried out by the public federal or cantonal authorities are regulated by the provisions of, respectively, federal administrative law (Article 25 DPA) or the administrative law of the canton concerned. It is beyond the scope of this study to give a detailed presentation of those remedies.

28 Article 15, paragraph 1 DPA: "Actions relating to protection of privacy are governed by Articles 28, 28a and 28l of the Civil Code." This reference also relates to provisional measures, Meier P., *Protection des données – Fondements, principes généraux et droit privé*, Bern 2011, p. 592, point 1826.

29 RS 231.1

30 RS 232.11

31 In respect of copyright, see Barrelet D. and Egloff W., *Le nouveau droit d'auteur*, Bern 2008, 3rd edition, p. 341, point 5 and Schlosser R., "Commentaire de l'art. 62", in de Werra J and Gilliéron P, *Propriété intellectuelle*, Bern 2013, p. 496 point 5; for trade mark law, Cherpillod I., *Le droit suisse des marques*, Lausanne 2007, p. 241 and Schlosser R., "Commentaire de l'art. 55", in de Werra J and Gilliéron P, *Propriété intellectuelle*, Bern 2013, p. 1121 point 4.

It follows that ISPs could be obliged by the civil courts to block access to sites infringing copyright or trade mark law.[32] I say "could" because there is at present no case law on this matter; this is primarily because the rights-holders have hitherto taken action directly against the persons violating intellectual property.[33]

A change of course might occur in the near future, following the presentation by the Government to the Parliament at the end of 2015 of a draft of modernization project for the Federal Copyright Act. This expressly provides for a procedure of *notice and take down* of materials which infringe copyright (see article 66d).[34] One should note that the Government insists in its explanatory report on the pressing need to avoid over-blocking and to only take action at the ISP level only at as a subsequent step (namely, if an intervention at the website host level turns out to be without success).[35]

2.1.1. Unfair competition

The purpose of the Federal Unfair Competition Act (hereafter the UCA[36]) is to combat business practices that are deceptive, abusive or in bad faith; in this connection, it focuses in particular on disparagement of competitors, false claims about the quality of a product, damaging comparative advertising, misleading price indications and commercial spamming (see Article 3 UCA for a non-exhaustive list[37] of the various contentious practices).

Article 9 UCA provides for actions to prevent or halt a violation of the Act.[38] These actions can be brought by a competitor or a consumer (where appropriate, professional organisations or consumer protection associations can bring them on their behalf), or exceptionally, by the Swiss Confederation.[39] The persons who can be cited as defendants, formerly restricted to economic operators, now includes anyone who, directly or indirectly, contributes to the infringement, including the media.[40]

Accordingly, ISPs could also be obliged by the civil courts to block access to sites infringing unfair competition law.

---

32 Final report of the Copyright Working Party AGUR12 of 28 November 2013 (hereafter the AGUR12 Report), Bern, p. 49 point. 3.14, and p. 78.

33 Ibid. p. 36.

34 See the Explanatory report of the Federal Council, 11 December 2015, p. 72.

35 Ibidem, p. 73.

36 RS 241.

37 Article 2 DPA contains a general clause worded as follows: "Any behaviour or business practice that is deceptive or that in any other way infringes the principle of good faith and which affects the relationship between competitors or between suppliers and customers shall be deemed unfair and unlawful".

38 "Whoever, through an act of unfair competition, suffers or is likely to suffer prejudice to his or clientele, his or her credit or his or her professional reputation, his or her business or his or her economic interests in general, may request that the courts a. prohibit an imminent prejudice, b. remove an ongoing prejudice".

39 The Swiss Confederation, represented by the Secretary of State for the Economy, can take action if collective interests are threatened or are breached (Art.10 (3) of the Federal Law on Unfair Competition).

40 Federal Supreme Court judgment 117 IV 193; see also Spitz P., "Commentaire de l'article 9", in Jung P. and Spitz P., *Bundesgesetz gegen Unlauter Wettbewerb*, Bern 2010, p. 695.

2.1.2. Criminal-law measures

These are of two kinds: preventive blocking and permanent blocking in addition to the penalty. In both cases, the measures is controversial as it is not based on any explicit legal provision, but rather on a broad interpretation of procedural or substantive criminal law relating to, respectively, seizure (Article 263 of the Criminal Procedure Code, hereafter CPC[41]) or the forfeiture of dangerous objects (Article 69 of the Criminal Code, hereafter CrC[42])[43]. Given that these two provisions refer specifically to items or objects, in other words tangible, physical assets, some authors reject their standing as a legal basis for ordering ISPs to block access to unlawful sites; in the absence of any legal basis, such restriction on the freedom of information could be deemed contrary to the Constitution.[44] **This controversy over whether blocking is compatible with the Constitution appears to have inhibited the criminal prosecution authorities which have rarely ordered such a measure**.

The few cases in this area have been predominantly in the canton of Vaud. In 2009 the Canton Court approved an order to block 11 IP addresses giving access to defamatory sites which were hosted abroad to deliberately circumvent Swiss law; the blocking order was issued to all ISPs based in Switzerland.[45] The courts ruled that such a measure was compatible with the Constitution arguing "a maiore ad minus" that as the prosecution authorities were entitled to physically seize the ISP servers to prevent access to the sites in question, they were all the more entitled to order the less restrictive measure of blocking.[46] In a subsequent judgment concerning a hosting services provider, the same court held that it was justified to equate blocking with seizure particularly as such a measure was in line with the spirit of the law, which should be interpreted in a dynamic way taking account of technological advances: "provisional, and then where necessary permanent, blocking of access to a blog containing defamatory statements is not fundamentally any different from seizure and then, where necessary, forfeiture and destruction of a collection of printed material containing defamatory statements. We do not therefore see any reason to deal with the first case differently from the second in which seizure with a view to forfeiture is undoubtedly possible."[47]

While the Swiss government would appear to concur with this approach,[48] the Federal Supreme Court still has to adopt a clear position on the matter. Admittedly, an appeal was lodged in the first case referred to in the preceding paragraph, but as the appellant, one of the ISPs concerned by the

---

41 RS 312.0.

42 RS 311.0.

43 "Items and assets belonging to an accused or to a third party may be seized if it is expected that the items or assets: a. will be used as evidence; b. will be used as security for procedural costs, monetary penalties, fines or damages; c. will have to be returned to the persons suffering harm; d. will have to be forfeited."

44 In particular, Schwarzenegger C., "Sperrverfügungen gegen Access-Provider – über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet", in Arter O. and Florian J. (eds), *Internet-Recht und Electronic Commerce Law*, Bern 2003, p. 249 et seq. A contrary view is taken by Moreillon L. and Parein-Reymond A, *Code de procédure pénale*, Basel; 2013, p 752 point 9.

45 Judgment of the Indictments Court of the Vaud Cantonal Court of 26 March 2009.

46 This "a maiore ad minus" reasoning was used for the first time in 2005, by the Federal Criminal Court in a case concerning the blocking of websites used to advertise and unlawfully sell therapeutic and medical products (Federal Criminal Court judgment of 16 February 2005, BV 2004.26).

47 Judgment of the Vaud Cantonal Court of 18 June 2014, forumpoenale 3/2015, p. 149 et seq., in particular recital 4d.

48 See the reply by the Federal Council to a question from Mr Schwaab (12.1128), of 13 February 2013: "If content which is prohibited by the law has any link to Switzerland, the prosecuting authorities can, by means of a decision, order that content to be seized (Article 263 CPC) blocked or removed, where the said content is used as evidence in the criminal proceedings, or be otherwise forfeited."

injunction in question, had lodged the appeal out of time, the Supreme Court did not examine the legality of the blocking measure.[49] In March 2015, the Federal Supreme Court, hearing an appeal against the blocking by the Valais criminal justice system of two sites containing defamatory accusations, left the question open, merely referring the case to the lower court to examine whether the conditions for blocking had been satisfied (in particular, the seriousness of the accusations made) and if such was the case, whether it was possible, in accordance with the principle of proportionality, to block access solely to the statements in question.[50]

However, in the fight against cybercrime, it is possible to order administratively the blocking of the domain name of a malicious website. The Ordinance on Internet Domains (hereafter the OID[51]) authorised the blocking via the "registry"[52] of a domain name subordinate to it, if there are serious suspicions that the site in question is used to access, by unlawful means, critical data belonging to a third party (phishing) or to distribute malicious software (malware);[53] the measure must be requested by an anti-cybercrime service recognised by OFCOM, the Federal Communications Office. The blocking shall last for 30 days, following which it must be confirmed by the Federal Office of Police (Article 15 OID). Such confirmation has the value of an administrative decision, subject to an administrative appeal in accordance with the customary rules for such matters.[54]

2.1.3. Administrative-law measures (national security, moral standards, etc.)

In the absence of any case law in this field, it is doubtful whether the administrative authorities are authorised to oblige ISPs to block websites where this cannot be based on a specific legal provision.

To date, there is only one norm expressly relating to the administrative blocking of IP addresses: Article 13 e.5 of the Federal Internal Security Act (hereafter ISA[55]). And even there, the blocking order has no binding effect. The Federal Office of Police can merely "recommend" that ISPs block access to sites containing propaganda material.[56] This approach has been adopted to obtain the blocking of websites used to disseminate jihadist propaganda from abroad.[57]

The aforementioned Article 13 ISA also codifies the general administrative practice with regard to blocking: an emphasis is placed on dialogue with the ISPs. The aim is to encourage ISPs, wary of any manipulation, to co-operate voluntarily; this has met with greater or lesser success depending on the

---

49 Federal Supreme Court judgment of 11 October 2009 (1B_242/2009).

50 Federal Supreme Court judgment of 19 March 2015 (1B 294/2014), recital 4.

51 RS 784.104.2. This text is based on a delegation of powers from the Parliament to the Federal Council contained in the Federal Telecommunications Act (RS 784.10), worded as follows: "The Federal Council may issue technical and administrative regulations for the security and availability of telecommunications infrastructures and services."

52 The registry, as defined in the annex to the OID, "means an entity charged with the central organisation, administration and management of a top-level domain, and with the allocation and revocation of rights of use of the domain names which are subordinate to it."

53 RS 784.104.2.

54 See Articles 44 et seq. of the Federal Administrative Procedure Act (RS 172.021).

55 RS 120.

56 Under the terms of Article 13 e.1 ISA, this refers to websites "whose content incites, in a serious and practical way, the use of violence against persons or objects".

57 See the reply from the Federal Council of 8 May 2015 to the question from Mr van Singer (15.1027, What preventive action does the Federal Council intend to take to avoid the implantation of forms of violent extremism in Switzerland?).

subject matter: the fight against child pornography is certainly the area in which this co-operation works best.[58]

Typical of this prudent and conciliatory approach adopted by the administrative authorities is the case of the Federal Gaming Board, which for a long time has sought to prevent access by Swiss Internet users to online casinos operating from abroad, offering services which are prohibited in Switzerland. In the absence of a legal basis explicitly authorising it to require ISPs to block access to these sites,[59] it has begun discussions on this matter with the country's main ISPs. As these talks proved unsuccessful, the government decided, as part of the complete revision of the Federal Gaming Act currently in progress, to insert a specific provision authorising the Federal Gaming Board to order the blocking of gaming sites located abroad. A black list of the sites in question will be regularly updated, forwarded to the ISPs for blocking, and then officially published.[60]

Furthermore, it should be noted that on the basis of the general public order clause (Article 36.1 (3) of the Federal Constitution), the authorities may take action without there being a legal basis against anyone who threatens public security. The threat must, nevertheless, be immediate and serious;[61] in addition, in order to comply with the principle of proportionality enshrined in sub-paragraph 3 of Article 36,[62] there must be no less intrusive possibilities for countering the danger.[63] As far as we are aware, no blocking order has yet been issued on the basis of this general public order clause.

2.2. Removal of unlawful content

2.2.1. Protection of personality rights and data protection

The actions based on Article 28 CC, either directly (protection of personality rights, see 2.1.1 above) or as the result of a referral (data protection, cf. 2.1.4) are a further way of obtaining the removal of unlawful content. These actions can be brought against anyone who "contributes" to the infringement, and the persons who can be cited as defendants include the hosting provider and social platform operators.

This was confirmed by the Federal Supreme Court which, in 2011, ordered the removal of a blog run by a Geneva newspaper, containing defamatory posts by a third party.[64] In their recitals, the judges clearly rejected submissions put forward by the defendant (the newspaper) calling for the victim to take action against the author of the statements in question and not the intermediary which had merely served as a means of disseminating them: "Similarly, the defendant is mistaken in claiming

---

58 See below 2.2.5

59 The Federal Gaming Board has repeatedly complained of this lack of legal basis, see for example its 2014 Annual Report, p. 19.

60 Article 84 of the draft of the Gaming Act (provided to Parliament in October 2014, FF 2015 7769): "1. Access to online gaming services must be blocked when such services are not authorised in Switzerland. 2. Such blocking shall apply exclusively to gaming services whose operator is based abroad and which are accessible in Switzerland. 3. The Federal Gaming Board and the inter-cantonal enforcement authority shall each hold a list of gaming services blocked in their field of competence and shall update this list on a regular basis. 4. Telecommunication service providers shall block access to the gaming services appearing on one or other of these lists."

61 Article 36 of the Federal Constitution provides that "restrictions on fundamental rights must have a legal basis. (…) The foregoing does not apply in cases of serious and immediate danger where no other course of action is possible." For a practical case, see the Federal Supreme Court judgment 126 I 118 (forced medical care of a patient in the absence of formal legal basis).

62 "Any restrictions on fundamental rights must be proportionate".

63 For further details, see Kiener R. and Kälin W., *Grundrechte*, Bern 2013, p. 110 et seq.

64 Federal Supreme Court judgment of 14 January 2013 (5A_792/2011).

that it would be impossible to constantly monitor the content of all the blogs hosted. These aspects, in particular the duty of attention and monitoring required of everyone, relate to the question of malicious intent which is not relevant in actions relating to personality rights."[65]

An action of this type can also be brought against a link provider. The latter may be obliged to delete a link to a site infringing personality rights, provided it is a direct link to the information at issue; a link which merely directs in a general way to a website portal which includes, amongst other things, defamatory statements, is not sufficient.[66]

2.2.2. Intellectual property and unfair competition

Actions relating to copyright, trade mark law and unfair competition can also be brought against a social network host or operator in view of the very broad range of persons who can be cited as defendants in such actions.[67] In the absence of any case-law in this area, reference is made to 2.1.3 and 2.1.4 above.

That said, it is appropriate to clarify that the draft reforms of the Federal Law on copyright of December 2015, already mentioned (see 2.1.3. of this report), introduce a notice and takedown procedure for content which infringes copyright (see article 66b).[68] In essence, the website host which learns from the owner of the copyright that, without the copyright owner's consent, access is being given to protected works, has to take them down. In doing so, the website host informs those responsible for posting the material in question of its takedown, thereby providing an opportunity for them to oppose such removal. In the case of opposition to the removal, the website host must restore access; it is then for the copyright owner to assert his claim before a civil judge.

2.2.3. Criminal law

The criminal prosecution authority may order the removal of content that is punishable under criminal law, either as a preventive measure by means of seizure or permanently by means of a forfeiture measure.

This removal is based on the provisions of the CPC and the CrC on seizure and forfeiture of tangible items and objects (see 2.1.5 above). It is the lower courts that have interpreted the law in this dynamic way; it still has to be confirmed by the Federal Supreme Court, particularly as some legal writers believe that a specific legal basis for such measures must be adopted.

2.2.4. Administrative law

The only specific authorisation to order the removal of unlawful content is to be found in the ISA. The Federal Office of Police may, following consultation of the Confederation, order the removal of a site hosted in Switzerland containing propaganda material (Article 13e.5 ISA). Contrary to what applies to ISPs (see 2.1.6 above), the injunction against hosting service providers or platform operators is binding (and not merely voluntary).

---

65 See also the Federal Supreme Court judgment of 28 October 2003 (5P.308/2003), removal of defamatory newspaper articles from a third party's personal website.

66 Federal Supreme Court judgment of 4 May 2015 (5A_658/2014), recital 4.2.

67 See in particular Schlosser R., "Commentaire de l'art. 62", in de Werra J. and Gilliéron P., *Propriété intellectuelle*, Bern 2013, p. 497 point 6; the author specifically refers to a case concerning the hosting provider of a site reproducing works infringing copyright.

68 See the explanatory report of the Federal Council of 11th December 2015, p. 71.

Given the physical proximity of hosting services to the content at issue, the question of whether or not it is lawful to have illicit content removed in the absence of any specific legal authority is less controversial than the question of the lawfulness of ordering sites to be blocked. Accordingly, some administrative authorities have had no hesitation in ordering removal simply on the basis of the general authorisation to deal with unlawful communications. For example, the Swiss Alcohol Board has obtained the removal of online alcohol advertising in violation of the Alcohol Act;[69] similarly, Swissmedic, the national medicines supervisory body, has taken action on numerous occasions against hosting services helping to disseminate prohibited advertisements of medicines.[70]

2.2.5. Self-regulation

On a purely voluntary basis, the SIMSA, the Swiss Internet Industry Association,[71] issued its Hosting Code of Conduct (HCC) on 1 February 2013. The aim of this Code is to compensate for the lack of any legal regulations on the civil and criminal liability of hosting services, establishing a notice and take-down (removal) procedure, which for more than ten years has been a feature of US law.[72] SIMSA members reserve the right, under the general conditions by which they are bound to their customers, to remove unlawful content brought to their attention.

To be admissible, the notice must contain at the very least the following information: name and address of the sender; (b) explanation of why the sender is particularly affected by the content (except in the case of offences prosecuted ex officio, such as child pornography); (c) URL of the offending web page or sub-page; (d) precise description of the allegedly unlawful content; (e) reason why the content is unlawful.[73] If the notice received fully satisfies these conditions and if it is highly likely[74] that it relates to unlawful content, the hosting services provider can block access to the site.[75] The customer will be informed of the blocking measure and of the reason why it was taken.[76] Lastly, failure to comply with the HCC results in a purely symbolic penalty: the hosting provider is no longer authorised to display the *Swiss quality hosting* seal of approval.

---

69 See Legal Basis for Social Media: Report of the Federal Council in fulfilment of the Amherd postulate 11.3912 of 29 September 2011, Bern 2013, p.61 point 5.4.1.

70 See in particular the judgment of the Federal Criminal Court of 16 February 2005, BV 2004.26; see also Junod V., *Publicité pour les médicaments: La santé publique l'emporte sur la liberté d'expression*, Medialex 2010, p. 10, footnote 24.

71 Internet platform operators are not members of SIMSA and consequently are not affected by these self-regulation measures.

72 See Section 512 (c) of the Digital Millennium Copyright Act.

73 Section 4.3 HCC.

74 "When assessing whether the notice is complete, whether a website should be blocked and whether legal proceedings should be instigated, the hosting provider applies the benchmark of a legal layman." (Section 7.3 HCC).

75 Section 7.1. HCC.

76 Blocking is not only provided for in the HCC, but is also mentioned in the contract between the hosting provider and its customer (the blocking procedure is described in the general terms and conditions appended to the contract). In contrast, neither the HCC nor the applicable contractual provisions refer to freedom of expression and the conditions under which this may be restricted.

3. Procedural matters

1.1. Actions based on civil law

These actions are regulated by the Code of Civil Procedure (hereafter CCP[77]). It follows that they may be ordered only by a judge ruling in the context of adversarial proceedings; an appeal can then be lodged with a higher court against the court decision. Unlike the situation in many European countries, the national data protection agency (the Federal Data Protection and Information Commissioner) has no decision-making power. If court action is contemplated, the victim must apply to the civil courts which have exclusive jurisdiction in this field (Article 15 DPA).

Moreover, blocking may be ordered on a provisional basis. In application of Articles 261 et seq. CCP, the court may take urgent, but temporary, measures against persons contributing to the infringement. These interim measures are, however, subject to stringent conditions in order to avoid any abuse: in particular it must be credibly shown that the victim will suffer harm that will be difficult to repair. As these interim measures could be equated to a form of prior censorship which would jeopardise freedom of information, the legislature restricted the action taken against "periodically published" media, such as (but not exclusively) the press, radio and television: in such cases, the courts are unable to order interim measures (for example an immediate ban on the broadcasting of a programme) unless the harm suffered by the victim is particularly serious and there is no manifest interest to be served by publication or broadcast (Article 266 CCP). While there is little doubt that an ISP or hosting provider cannot be considered as a media, as neither exercises any editorial supervision of the information, the same cannot be said of online platform operators. Nonetheless, the Federal Supreme Court refused to apply Article 266 CCP to a social network operator.[78] As a general rule, the court will hear the defendant before ordering any interim measures; it may however act without a hearing "In cases of special urgency, and in particular where there is a risk that enforcement of the measure will be frustrated" (ex parte interim measures), Article 265 CCP).

1.2. Criminal-law measures

Provisional blocking (or removing) – which, it will be recalled, is controversial as it is based on a dynamic interpretation of the seizure procedure (Article. 263 CPC[79]) – is a compulsory measure ordered by the authority conducting the investigation (the prosecution service); the person against whom the measure is taken is not heard beforehand. The seizure order may be appealed against before a court (the compulsory measures court) in accordance with Article 393 et seq. CPC. It should be noted that seizure is subject to the general principles governing compulsory measures; under the terms of Article 197 CPC, such measures may be taken only if "a) they are permitted by law, b) there is reasonable suspicion that an offence has been committed, c) the aims cannot be achieved by less stringent measures and d) the seriousness of the offence justifies the compulsory measure."

Just as controversial as provisional blocking (it is based on an equally dynamic interpretation of forfeiture), permanent blocking (or removal) is an ancillary measures to the sentence delivered by the court. Provided that the forfeited object has been used to commit the offence, forfeiture may be

---

77 RS 272.

78 Federal Supreme Court judgment of 4 May 2011 (5A 790/2010 recital. 5.2), refusal to consider a social network as belonging to the periodically published media; however, the Federal Supreme Court failed to explain the reasons for not considering a social network as a periodically published media body. See also the Federal Supreme Court judgment of 10 October 2013 (1C_335/2013), a blogger prohibited from filming the public sittings of a municipal council meeting for lack of any journalistic authority.

79 Cf. 2.1.5. above.

ordered against a third party who has not been a party to the trial[80] (which is the most frequent scenario in cases of permanent blocking involving an ISP or a hosting provider). Out of respect for the right to be heard, the court must, in such cases, summon the person against whom the measure is ordered.[81] Permanent blocking can be appealed against before the higher criminal court.

1.3. Administrative-law measures

In the (rare) cases where blocking or removal is the result of action taken by an administrative authority, such measures are ordered by administrative decision,[82] which must comply with the formal and specific conditions laid down in the Federal (or where appropriate Cantonal) Administrative Procedure Act, which can be subject to appeal. In particular, the person against whom the measure is taken has the right to be heard. In this regard, the Internal Security Act specifically provides that decisions to remove propaganda material (cf. 2.2.4 above) are governed by the Federal Administrative Procedure Act (Article 13e.2 ISA).

There is a particular procedure for the blocking of a domain name by means of the "register" (cf. 2.1.5 above). The blocking, as such, is carried out simply at the request of an anti-cybercrime service recognised by OFCOM; under the terms of Article 15.4 OID, the holder of the domain (and not the register) may refer the matter to the Federal Office of Police which will confirm (or not) the blocking by means of an administrative decision, which can be appealed against.

4. General Internet monitoring

1.1. Monitoring by the public authorities

There is no public entity in Switzerland tasked with the general and systematic monitoring of Internet content.

In the criminal-law field, however, the National Cybercrime Co-ordination Unit (CYCO) was set up in 2001. This is a body attached to the Federal Office of Police, tasked with carrying out detailed analysis of developments in online crime and, to this end, to search the Internet for content which is punishable under criminal law. In practice, the emphasis is placed on child pornography, racist propaganda and hate speech, and economic crime. If it identifies any offence, it refers the matter to the competent prosecuting authority (at cantonal or federal level, depending on the type of offence) to initiate a formal investigation. The CYCO holds a list of the main criminal sites abroad; this list is forwarded to ISPs with a recommendation that access to those sites be blocked. This type of voluntary collaboration with ISPs is viewed as positive.[83] In the fight against child pornography, the ISPs have even undertaken to block access on request from the CYCO:[84] their general terms and conditions make explicit provision for this measure. Each year, several hundred thousand attempts to

---

80 Hirsig-Vouilloz M., "Commentaire à l'art. 69 CP", in Roth R. and Moreillon L, *Code pénal I*, Basel 2009, p. 722 point 36.

81 Hirsig-Vouilloz M., ibid, p. 737 point 43 and the case law quoted in footnote 100. If the forfeiture is carried out independently of a criminal procedure, the forfeiture will be ordered by the public prosecutor who shall give the person concerned the opportunity to respond (Article 377 CPC). The order can be appealed against (Article 393 et seq. CPC).

82 Legal Basis for Social Media: Report of the Federal Council in fulfilment of the Amherd postulate 11.3912 of 29 September 2011, Bern 2013, p. 49 point 4.5.7.2 and p. 61 point 5.4.1.

83 CYCO 2014 annual report p. 111.

84 2007 Agreement between the CYCO and the main Swiss ISPs.

call up pages containing unlawful content have been blocked,[85] in the majority of cases following notifications from Internet users (and to this end CYCO makes available a form for flagging up dubious content).

1.2. Monitoring by Internet Service Providers

To date, no legal provision obliges ISPs to monitor the content they host and/or the sites to which they provide access. Does this mean that ISPs are exempt from any control obligations? The vast majority of legal writers believe that this is the case.[86] The case law too would appear to corroborate this, according to the only Federal Supreme Court judgment in this field, relating to the operator of a discussion forum; the operator was not found to be at fault for not having constantly monitored the hate-filled contributions of third parties posting on the forum in question: "It is inevitable that in running a discussion forum there is the risk of unlawful comment being posted there and, therefore, that interests that are legally protected by criminal law will be harmed. While, in itself, this risk is no greater than what is tolerable in society (Sozialadäquanz) and **most probably is not sufficient to impose an obligation of permanent monitoring**, the situation is, however, different when the operator of a forum is actually aware of the unlawful content on his site."[87]

5. Evaluation in the light of the case law of the European Court of Human Rights

As we have seen, the legal system in Switzerland governing the blocking and removal of unlawful content falls mainly under ordinary law. However, this does not fail to raise questions and doubts as to its compatibility with the standards laid down by the European Court of Human Rights with regard to restrictions on freedom of information. In the absence of any specific legal basis, upholding the requirements of the **clarity and foreseeability of the rule** required to establish interference leaves much to be desired. It is to be hoped that parliament, which has at last decided to tackle the question of defining the responsibilities of ISPs (cf. 1 above) will soon provide the necessary clarifications, as has been requested by, amongst others, the Federal Supreme Court, which thus far has refused to make up for shortcomings in legislation: "it is for the legislative, not the judiciary, to remedy the "serious consequences" for the Internet and for blog hosts to which the application of the law as it currently stands could give rise."[88]

In particular, it is essential to eliminate the considerable uncertainty over whether or not it is possible to order ISPs, who monitor neither directly nor indirectly the information conveyed via their services, to block access to unlawful content. The necessary clarifications relate to blocking under not only criminal law or administrative law, but also civil law. The general provisions on which it is based (Article 28 CC, Article 62 FCA, Article 15 TMPA and Article 9 UCA[89]) date from the pre-Internet age; their scope must be revised in line with the role played by the various intermediaries who help facilitate communication on the Worldwide Web.

---

85 Legal Basis for Social Media: Report of the Federal Council in fulfilment of the Amherd postulate 11.3912 of 29 September 2011, Bern 2013, p.62 point 5.4.2.

86 See, in particular, Fountoulakis C. and Francey J., *La diligence d'un hébergeur sur Internet et la réparation du préjudice*, Medialex 2014, p. 181.

87 Federal Supreme Court judgment of 2 May 2008 (6B 645/2007), in particular recital 7.3.4.4.2

88 Federal Supreme Court judgment of 14 January 2013 (5A_792/2011, recital 6.3).

89 Cf. 2. above.

Nonetheless, it must be pointed out that the administrative authorities and the prosecution bodies are aware of the precarious nature of the current system: in their relationship with ISPs, they have very rarely sought to impose blocking measures, but rather have opted for **dialogue**, attempting to persuade ISPs to prevent access on a voluntary basis. While this approach is to be welcomed, one cannot but express some reservations as to its compatibility with the requirements of the European Court of Human Rights as regards the enforceability of measures restricting fundamental freedoms: in the absence of any formal decision, it becomes impossible to appeal against wrongful blocking.

Lastly, like all fundamental freedoms, freedom of expression can be restricted only on three specific conditions, explicitly laid down in Article 36 of the Federal Constitution: **the restriction must have a legal basis, must be justified in the public interest and must be proportionate**. This last condition, in particular, is looked at very closely by the courts, as evidenced by their constant wish to avoid overblocking or to order blocking only where it is impossible to take action in Switzerland against the author or hosting provider.[90] The same is true of the legislature; Article 197 of the Criminal Procedure Code emphasises that compulsory measures (a category covering blocking or preventive removal[91]) must be applied not only as a last resort (priority must be given to less stringent measures where such are possible) but also with "particular caution" in respect of persons not accused of an offence, such as hosting providers and ISPs.

Bertil Cottier
15 December 2015

Revised on 03.05.2016 taking into consideration comments from Switzerland on this report

90 Cf. 2.1.1. above.

91 Cf. 2.1.5. above.