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 472-489

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.

MONACO

The Principality of Monaco has **no specific legal rule applying across the board to all sectors** regarding the blocking, filtering or removal of unlawful Internet content, but there are several laws providing a framework to implement such measures.

1. Sources

As there is no legal rule covering all sectors with regard to the blocking, filtering or removal of unlawful Internet content, Monegasque legislation is fragmented, and the use of the Internet is regulated by rules specific to several areas. Some constitute the transposition of the Principality's international commitments, while others are the result of national initiatives. Several draft Acts that might cover measures to block, filter or remove content have been tabled with the Bureau of the Monegasque parliament and are waiting to be dealt with.

In the Council of Europe context, the Principality of Monaco has ratified the European Convention on Human Rights of 1950,[1] the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and its Additional Protocol regarding supervisory authorities and transborder data flows of 2001[2] and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 2007[3] and signed the Convention on Cybercrime of 2001.[4]

The **Monegasque Constitution**[5] protects freedom of expression (Article 23) and private life (Article 22).

---

1 Act No. 1304 of 3 November 2005 approving the ratification of the Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, and of its Protocols 6, 7 and 13, Monaco Gazette of 11.11.2005, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/FD50CA566066E39AC125773F003D375D!OpenDocument (accessed on 17 September 2015).

2 Act No. 1354 of 4 December 2008 approving the ratification of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol regarding supervisory authorities and transborder data flows, Monaco Gazette of 12.12.2008, available (in French only) at http://www.legimonaco.mc/305//legismclois.nsf/ViewTNC/10C35BA7D2D3189BC125773F003DA840!OpenDocument (accessed on 17 September 2015).

3 Order No. 5209 of 20 February 2015 giving effect to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Monaco Gazette of 27 February 2015, available (in French only) at http://www.legimonaco.mc/305//legismclois.nsf/ViewTNC/5423E74340B58418C1257DFF00306780!OpenDocument (accessed on 17 September 2015).

4 Act No. 1402 of 5 December 2013 approving the ratification of the Council of Europe Convention on Cybercrime, Monaco Gazette of 20 December 2013, available (in French only) at http://cloud.gouv.mc/Dataweb/jourmon.nsf/9bf97b0da6308cfdc12568c40037f873/562ba4949dd7f255c1257c470039e09c!OpenDocument (accessed on 22 September 2015). This Act will enable the ratification of the Council of Europe Convention on Cybercrime if the Draft Act on Combating Technological Crime of 24 February 2015 No. 934 is adopted (see for example paragraph 2.2.5 of this opinion for a presentation of this draft act); the latter is designed to upgrade the Monegasque legislation in order that it complies with the Convention on Cybercrime before its ratification.

5 Constitution of the Principality, 17 December 1962 (amended on 2 April 2002), available at http://en.gouv.mc/Government-Institutions/Institutions/Constitution-of-the-Principality (accessed on 21 September 2015).

The **Digital Economy Act of 2 August 2011**[6] transposes Articles 12, 14 and 15 of European Directive 2000/31/EC on electronic commerce of 8 June 2000 by regulating the liability of technical service providers.[7]

The Protection of Personal Data Act, Act No. 1165 of 23 December 1993,[8] **as amended by the Act of 4 December 2008**,[9] **regulates the processing of personal data**. Section 18 has been declared unconstitutional by the Supreme Court of Monaco. The **Act** of 1st December 2015 **amending Sections 18 and 19 of Act No. 1165**[10] modifies the Act to bring it into conformity with the Constitution.

The Act **of 26 December 2007 on harsher penalties for crimes and offences against children**[11][12] inserted Article 294-4 into the Criminal Code. This obliges operators or service providers responsible for the operation of telecommunications and electronic communications networks and services and their staff to prevent public access to images or representations notified to them as constituting child pornography.

---

6 Digital Economy Act, Act No. 1383 of 2 August 2011, Monaco Gazette of 12 August 2011, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/D3F606E03CE7C5E0C125790B002F41BC!OpenDocument (accessed on 17 September 2015).

7 Title IV of the Digital Economy Act of 2 August 2011 transposes Articles 12, 14 and 15 of Directive 2000/31/EC on electronic commerce, of 8 June 2000; source: Draft Digital Economy Act No. 883 of 14 February 2011, p. 20, available (in French only) at http://www.conseil-national.mc/index.php/textes-et-lois/lois/item/253-1383-loi-sur-l-economie-numerique (accessed on 28 September 2015). Technical service providers are Internet access providers and hosting providers.

8 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/28A1A1D90812E249C125773F003BEEBB!OpenDocument (accessed on 17 September 2015). For details on processing operations that fall within the scope of this Act, see Sections 24 to 25.

9 Act No. 1353 of 04 December 2008 amending Act No. 1165 of 23 December 1993 regulating the processing of personal data, Monaco Gazette of 12 December 2008, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/8B15ED72C019E70CC125773F003DA7FF!OpenDocument (accessed on 17 September 2015).

10 Act No. 1420 of 1st December 2015 amending Sections 18 and 19 of the Protection of Personal Data Act No. 1165 of 23 December 1993, available (in French only) at http://www.conseil-national.mc/index.php/textes-et-lois/projets-de-loi/item/432-939-projet-de-loi-portant-modification-des-articles-18-et-19-de-la-loi-n-1165-du-23-decembre-1993-relative-a-la-protection-des-informations-nominatives.

11 Act no. 1344 on harsher penalties for crimes and offences against children, of 26 December 2007, Monaco Gazette of 28 December 2007, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/51DBAB282624E526C125773F003D867D!OpenDocument (accessed on 17 September 2015).

12 The explanatory memorandum of the private member's bill of 28 March 2006 on harsher penalties for crimes and offences against children makes no reference to the Council of Europe's 2007 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse; private member's bill available (in French only) at http://www.google.be/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB8QFjAAahUKEwiKvvGaqf7HAhXHEywKHfOyBwE&url=http%3A%2F%2Fwww.conseil-national.mc%2Findex.php%2Ftextes-et-lois%2Fpropositions-de-loi%2Fitem%2Fdownload%2F100_51e36bf1c32c13f5e806b3d8092d4432&usg=AFQjCNGlQVn617nf6fHqBEEQDpBIxFmu6w (accessed on 17 September 2015). However, the Act of 26 December 2007 on harsher penalties for crimes and offences against children would enable the application of the UN General Assembly's Optional Protocol on the sale of children, child prostitution and child pornography, adopted on 25 May 2000, which Monaco signed on 26 June 2000 and the ratification of which was authorised by Act No. 1335 of 12 July 2007, Monaco Gazette of 20 July 2007.

The "Justice and Freedom" Act of 26 December 2007[13] inserted into the Code of Criminal Procedure provisions on special investigation techniques in connection with correspondence sent by means of electronic communications.[14]

The **Act of 15 July 2005 on freedom of public expression**[15] criminalises the abuse of freedom of expression. It enables liability to be imposed on authors, distributors, poster display firms and sellers but does not expressly refer to the liability of Internet players.

The **Terrorism Act of 29 June 2006**[16] contains no provisions specifically relating to the use of the Internet.[17]

A **Draft Act on Combating Technological Crime**[18] has been tabled in order to complete the process of bringing Monegasque law into line with the Convention on Cybercrime. At the time of writing, this draft is before parliament. It contains criminal-law provisions and provisions of criminal procedure relating to blocking, filtering, deleting, searching for and seizing computer data.

A **Draft Act on the Electronic Trade in Medicines** and on Group Purchasing Entities[19] will amend the Pharmacy Practice Act, Act no. 1029 of 16 July 1980. There are currently no provisions governing Internet sales of medicines.

Intellectual property is governed by the Protection of Literary and Artistic Works Act of 24 November 1948,[20] the Patents Act of 20 June 1955,[21] the Designs and Models Act of 20 June 1955[22] and the

---

13 "Justice and Freedom" Act, Act No. 1343 of 26 December 2007 amending certain provisions of the Code of Criminal Procedure, Monaco Gazette of 28.12.2007, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/6610017E5BEEAEF9C125773F003D8653!OpenDocument (accessed on 21 September 2015).

14 Code of Criminal Procedure, Articles 106-1 to 106-11.

15 Act on Freedom of Public Expression, Act No. 1299 of 15 July 2005, Monaco Gazette of 22 July 2005, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/29AD7325E3A152A4C125773F003D2E4E!OpenDocument (accessed on 22 September 2015).

16 Terrorism Act, Act No. 1318 of 29 June 2006, Monaco Gazette of 7 July 2006, available at http://www.siccfin.gouv.mc/364/wwwnew.nsf/c3241c4782f528bdc1256d52004f970b/7ee61b6f6821575bc12571bd002a9a4e!OpenDocument (accessed on 22 September 2015).

17 The Principality of Monaco is not a party to the 2005 Council of Europe Convention on the Prevention of Terrorism but has ratified the 1977 European Convention on the Suppression of Terrorism.

18 Draft Act on Combating Technological Crime, Act No. 934, of 24 February 2015, available (in French only) at http://www.conseil-national.mc/index.php/textes-et-lois/projets-de-loi/item/411-934-projet-de-loi-relative-a-la-lutte-contre-la-criminalite-technologique (accessed on 17 September 2015).

19 Draft Act on the Electronic Trade in Medicines and on Group Purchasing Entities, Act No. 937, available (in French only) at http://www.conseil-national.mc/index.php/textes-et-lois/projets-de-loi/item/430-937-projet-de-loi-relative-au-commerce-electronique-de-medicaments-et-aux-structures-de-regroupement-a-l-achat (accessed on 24 September 2015).

20 Act on the Protection of Literary and Artistic Works, Act No. 491, of 24 November 1948, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/9A89A5695632E537C125773F0037DFB2!OpenDocument (accessed on 23 September 2015).

21 Patents Act, Act No. 606 of 20 June 1955, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/7ED535A7D81C73FCC125773F0038111F!OpenDocument (accessed on 23 September 2015).

22 Designs and Models Act, Act No. 607 of 20 June 1955, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/56789D461A336459C125773F00381189!OpenDocument (accessed on 23 September 2015).

Trademarks and Service Marks Act of 10 June 1983.[23] These Acts have not been updated with regard to the protection of intellectual property on the Internet and do not deal with issues of blocking or removing Internet content that infringes intellectual property rights. Nor has our research enabled us to identify a general provision that would allow a civil court to issue an injunction to halt or prevent an infringement.[24] Intellectual property will consequently not be discussed any further in this opinion.

There is a legal vacuum as far as **online gaming** is concerned. The Gaming Act of 12 June 1987,[25] the Ministerial Order of 26 July 1988 regulating games of chance [26] and the Order on the municipal police of 11 July 1909[27] have not been amended to adapt the legislation to the development of online gaming. This was planned to be done by means of a draft Act amending the Gaming Act of 12 June 1987[28] but the draft was withdrawn in 2006. Consequently, it will not be possible in this opinion to assess measures to block, filter and remove content relating to online gaming.

It emerged from our discussions with the Monegasque authorities that several pieces of legislation that are potentially relevant in connection with blocking, filtering and removing Internet content are currently being drafted and could be enacted in 2016. **The aforementioned draft Acts and other instruments, the content of which was not communicated to us, would modernise Monegasque law**.

2. Applicable regulations

2.1. Blocking and/or filtering of unlawful Internet content

Measures for blocking and filtering unlawful Internet content are laid down in legal rules specific to each field and relate to various players.

2.1.1. Liability of Internet access providers

The Digital Economy Act of 2 August 2011 (hereinafter "the 2011 Act"), and more specifically Title IV on the liability of technical service providers, governs the liability of Internet access providers**.**

---

23 Trademarks and Service Marks Act, Act No. 1058 10 June 1983, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/41A02BE7F2220723C12578C4002D2522!OpenDocument (accessed on 23 September 2015).

24 See, however, the interlocutory procedure provided for by Article 414 of the Code of Civil Procedure.

25 Gaming Act, Act No. 1103 of 12 June 1987, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/9481C4AFB3115DC4C125773F003BBA6E!OpenDocument (accessed on 29 September 2015).

26 Ministerial Order No. 88-384 of 26 July 1988 regulating games of chance, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/74C730DD081DCF37C125773F003BC11A!OpenDocument (accessed on 22 September 2015).

27 Order on the municipal police of 11 July 1909, available (in French only) at http://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/FA9CE7A1111010D7C125773F00376E62!OpenDocument (accessed on 22 September 2015).

28 Draft Act No. 722 amending the Gaming Act, Act No. 1103 of 12 June 1987, available (in French only) at http://www.conseil-national.mc/index.php/textes-et-lois/projets-de-loi/les-projets-de-loi-retires/item/31-722-projet-de-loi-modifiant-la-loi-numero-1103-du-12-June-1987-relative-aux-jeux-de-hasard (accessed on 29 September 2015).

Section 31 states: "the service provider […] that provides access to a communication network cannot be held **civilly or criminally liable on account of [information supplied by a service recipient] except in circumstances in which they have either originated the request for the transmission at issue or selected the recipient of the transmission".**

The Act also states that the service provider **shall inform its subscribers about the existence of technical means enabling them to restrict access to certain services** or to select such services, and to prevent any act of counterfeiting carried out on a communication network, and shall offer them at least one of those technical means (Section 31 of the 2011 Act).

In addition, Section 34 of the 2011 Act imposes on Internet access providers, as well as on hosting providers, the obligation to retain data that could identify anyone who has contributed to the creation of the content or part of the content of the services they provide.

2.1.2. Protection of personal data

The Personal Data Protection Act of 23 December 1993, as amended by the Act of 4 December 2008 (hereinafter "the amended 1993 Act") **requires data controllers to set up a system preventing the leakage of personal data**. This involves restricting processing accessibility to certain individuals. Section 17 of the Act provides, for example: "The data controller or his/her representative shall implement appropriate technical and organisational measures to protect personal data against […] unauthorised disclosure or access. […]. Where the data controller or his/her representative makes use of the services of one or more service providers, he/she shall ensure that the latter are able to comply with the [data protection] obligations".

The Monegasque Data Protection Authority (CCIN)[29] has published a **practical guide**[30] for people who process personal data on making such data secure.

2.1.3. Penalties for crimes and offences against children

The Act of 26 December 2007 on harsher penalties for crimes and offences against children (hereinafter "the 2007 Act") inserted provisions into the Criminal Code **making it a criminal offence to commit certain acts against children via the Internet** and lays down **obligations for Internet service providers** to block and remove such content.

This Act does not systematically and explicitly provide for measures to block, filter or remove content for each of the offences mentioned, but its criminalisation of specific acts can serve as a basis for the possible introduction of such measures, as provided for by the Digital Economy Act of 2 August 2011 on the liability of Internet service providers (see points 2.1.1. and 2.2.1. of this report).

Various offences have been established in Monegasque legislation in order to protect children when using the Internet.[31]

---

29 The CCIN is an independent Monegasque administrative authority. Its powers are set out in Section 2 of Act No. 1165 of 23 December 1993, as amended, on the protection of personal data.

30 CCIN, *Sécurisez vos fichiers* (Secure your files), available (in French only) at http://www.ccin.mc/publications/guides/document/securisez-vos-fichiers.pdf (accessed on 28 September 2015).

31 Article 266 of the Criminal Code increases the prison sentence imposed when, in order to attempt, prepare, commit or encourage or facilitate an offence against public decency, acts leading to the corruption of minors, the organisation or facilitation of the sexual exploitation of minors (Article 265 of the Criminal Code), "the minor has been in contact with the offender by means of an electronic

For example, Article 294-3 of the Criminal Code provides for penalties for several acts relating to **child pornography:**[32] procuring or transmitting an image or pornographic representation of a minor, knowingly offering or distributing such an image or representation by whatever means, the deliberate possession of such an image or representation, and knowingly accessing such an image or representation. Moreover, prison sentences and fines are increased when an electronic communications network has been used to distribute an image or representation of a minor to a non-specified audience.

Only this article has a provision that expressly provides for content-blocking measures. Article 294-4 of the Criminal Code provides: "when the images or representations referred to in Article [294-3 of the Criminal Code] have been brought to their knowledge in connection with their professional work, **operators or service providers responsible for operating networks and telecommunications and electronic telecommunications services, or one of their staff, shall carry out the necessary operations to prevent public access to such images** and make them available to the judicial authority for the detection, investigation, and prosecution of criminal offences". These measures to prevent access to the images concerned may correspond to the **measures to block or remove content** that are the focus of this study. If they fail to comply with this obligation, Internet access providers face prison sentences and fines.

---

communications network to distribute messages to a non-specified audience" (Article 266 2° of the Criminal Code).

Article 294-5 of the Criminal Code makes it a punishable offence to force a minor to view pornographic scenes or performances.

Article 294-6 provides for the punishment of attempts to lure minors for sexual purposes through the use of electronic communications and increases the penalty when a meeting has taken place.

Article 294-7 establishes penalties for the dissemination, by whatever means and using whatever medium, of a message of a violent or pornographic nature or one that offends against human dignity when the message is addressed to minors.

32 The offences referred to in Article 294-3 of the Criminal Code are considered to have been committed when they involve a minor, a person whose physical appearance is that of a minor if it has not been established that that he or she was at least eighteen years of age at the time, and when the image is "realistic", by which is meant a manipulated image of an individual created wholly or partly by digital means (Article 294-3, paragraph 7, of the Criminal Code).

2.1.4. Draft Act on the electronic trade in medicines

A draft Act on the electronic trade in medicines and on group purchasing associations seeks to introduce into Monegasque law a legal framework based on French legislation. This framework would adopt the following principles: "only medicines supplied without a prescription may be offered for sale online; only genuine pharmacies duly authorised by the Minister of State after obtaining the opinion of the Council of the Order of Pharmacists shall be able to operate an Internet site for the online sale of medicines; in order to operate a website, pharmacist shall be required to comply with the rules of good practice and provide certain specific information aimed at informing consumers, with the aim of making their Internet purchases safe and secure".[33]

Where these principles are not complied with, the draft Act proposes **authorising the Minister of State to close down the Internet site temporarily**, for a period not exceeding five months, at the end of which the **authorisation to operate that site could be revoked** if the pharmacist has still failed to comply with the rules applicable. The draft Act does not provide for the creation of a body to monitor the Internet trade in medicines.

2.2. Removal of unlawful content from the Internet

Measures for removing unlawful Internet content are set out in legal rules specific to each field and relate to various players.

2.2.1. Liability of hosting providers

The Digital Economy Act of 2 August 2011, in particular Title IV on the liability of technical service providers, states that **hosting providers** can be held **civilly or criminally liable for the storage of unlawful activity or information only if they were aware of their unlawful nature** or of any facts and circumstances making this unlawful nature obvious and if, as soon as they became aware of that unlawful nature, they did not **act promptly to remove the information or make access to it impossible** (Section 29 of the 2011 Act).

Section 29 of the 2011 Act provides that this knowledge **is assumed to have been acquired when the following elements have been notified to the hosting provider**: "the date of the notification; if the notifier is an individual: his or her surname, first names, occupation, place of residence, nationality, date and place of birth; if the requester is a legal entity: its corporate form, its name, its registered office and legal representative; the name and address of the recipient or, in the case of a legal entity, its name and registered office; a description of the facts at issue and their precise location; the reasons why the content must be removed; a copy of the message addressed to the author or publisher of the information or activities at issue requesting their interruption, removal or modification, or the reasons why the author or publisher could not be contacted".

Section 30 of the 2011 Act sets out the penalties for **wrongful denunciation** by providing for a prison sentence of six to twelve months and a fine of €9,000 to €18,000 "for anyone who, despite being aware of the inaccuracy of the information, informs the service provider […] that content or an activity is unlawful with the aim of obtaining its removal or preventing its dissemination".

In order to facilitate any subsequent identification in the event of legal proceedings being brought against unlawful content, **the persons whose job it is to maintain an online public communication**

---

[33] Draft Act on the electronic trade in medicines and on group purchasing organisations, No. 937, explanatory memorandum, paragraph 14.

service must make available to the public the details necessary for their identification (Section 33 of the 2011 Act).

Section 34 imposes on hosting providers, as well as on Internet access providers, the obligation to **retain data that could identify anyone who has contributed to the creation of the content or part of the content** of the services they provide.

Technical service providers (both hosting providers and Internet access providers) could in addition **be held liable if they select or modify the information they store** or **if they have either originated the request for the transmission in issue or selected the recipient of the transmission** (Section 31 of the 2011 Act).

2.2.2. Protection of personal data

Data that may not be processed are specified in Chapter II of the Personal Data Protection Act of 23 December 1993, as amended. The Act also details the **procedural rules** to be complied with for processing data that may lawfully be collected. In the event of failure to comply with one of these rules, **the data must be withdrawn from the processing or the processing must be discontinued**.

In particular, no use may be made of data concerning opinions or political, racial or ethnic, religious, philosophical or trade union affiliations or data relating to a person's health, including genetic data, to his or her sex life or lifestyle or to measures of a social nature, with strictly defined exceptions (Section 12 of the amended 1993 Act).

The processing of public security-related data, such as data on breaches of the law, convictions or security measures, or relating to the prevention, detection, investigation and prosecution of criminal offences, to the execution of criminal convictions or to security measures may only be carried out **by the judicial and administrative authorities** within the limits of their remit (Section 11 of the amended 1993 Act).

The amended 1993 Act, also provides that, apart from the reasons set out above, data may be **removed at the instigation of the data controller or at the request of the data subject**.

Section 15-2 of the amended 1993 Act provides that **the data controller or his or her representative shall, in particular, take appropriate steps to delete automatically any information obtained by fraudulent, unfair or unlawful means and to delete identifying data upon expiry of the storage period specified**. The CCIN has published two **guides** to disseminate this information both in the public sector and among assimilated bodies[34] and in the private sector.[35]

Section 16 of the amended 1993 Act enables **the data subject to demand that information concerning him or her be rectified, supplemented, clarified, updated or deleted if it proves inaccurate, incomplete, ambiguous or obsolete or if its collection, recording, disclosure or storage**

---

34 CCIN, *Soumettez vos traitements* (Submit your processing operations), aimed at the public sector and assimilated bodies, available (in French only) at http://www.ccin.mc/publications/guides/document/soumettez-vos-traitements.pdf (accessed on 28 September 2015).

35 CCIN, *Déclarez vos données* (Declare your data) aimed at the private sector, available (in French only) at http://www.ccin.mc/publications/guides/document/declarez-vos-donnees.pdf (accessed on 28 September 2015).

is prohibited. In this connection, the CCIN has published a **guide**[36] to inform people whose personal data are processed, and especially about the right of deletion.

In the event of failure to comply with the above provisions, **the CCIN or a court may order the deletion of the data**, or even the discontinuation of the processing operation (see point 3.1. of this report).

In the event of failure to comply with an obligation to delete information, Sections 21 and 22 of the amended 1993 Act provide for **prison sentences and fines**.

Section 23 of the same Act provides that **"the court also has the power to order the forfeiture and destruction, without compensation, of media containing infringing personal data."**

2.2.3. Penalties for crimes and offences against children

Reference is made here to point 2.1.3. of this report as the analysis therein of the Act of 26 December 2007 on harsher penalties for crimes and offences against children in connection with providing a legal basis for measures to block and filtering content also applies, *mutatis mutandis*, to measures to remove unlawful Internet content.

2.2.4. Abuse of freedom of expression

Monegasque law does not have a concrete disposition for the blocking, filtering or removal of content abusing freedom of expression on the Internet.

However, the Act of 15 July 2005 on freedom of public expression criminalizing abuse of freedom of expression (for example: incitement to crimes and offenses, and especially to the commission of acts of terrorism, the provocation of hatred or violence, the obscenity, the defamation, the insults , etc.), it may be asked to hosting providers to remove such content , since they are illegal, under penalty of engaging their responsibility (Article 29 of the Act of 2 August 2011 on the digital Economy ; see paragraph 2.2.1 of this report).

2.2.5. Draft Act on combating technological crime

The draft Act on combating technological crime provides that in a search as part of a **judicial investigation**, the **public prosecutor may order the permanent deletion of computer data whose retention or use is unlawful or constitutes a danger to the safety of persons or property**, after a copy has been made for purposes of the investigation (proposed Article 255 of the Code of Criminal Procedure).

Moreover, the draft Act will lay down other **obligations applying to operators and providers of services responsible for the operation of telecommunications and electronic communications networks** and **designed to protect individual privacy and, more precisely, personal data**. These obligations correspond to the requirement to remove content since information held must be deleted or, at the very least, may not be used.

First of all, Section 2 of the draft Act will insert Article 389-11-1 into the Criminal Code in order to impose an **obligation to delete or anonymise any traffic data**[37] on operators and providers of

---

36 CCIN, *Protégez votre identité* (Protect your identity), available (in French only) at http://www.ccin.mc/publications/guides/document/protegez-votre-identite.pdf (accessed on 28 September 2015).

services responsible for the operation of telecommunications and electronic communications networks and services. However, the draft Act provides for the following **exceptions** to this obligation: "for the purposes of the detection, investigation, and prosecution of criminal offences and with the sole aim of enabling, where necessary, information to be made available to the judicial authority, a postponement of a maximum of one year may be granted for operations to delete or anonymise certain categories of technical data".[38] An exception may also be made for the purposes of billing and paying for electronic communications services[39] and, with the customer's consent, for business purposes.[40] Finally, certain data may be retained to ensure network security.[41]

The proposed Article 389-11-4 of the Criminal Code lays down conditions concerning the location of a user's terminal equipment: "notwithstanding the provisions of Articles 389-11-2 and 389-11-3 [presented in the previous paragraph of this report] and subject to the requirements of judicial investigations, **data enabling the user's terminal equipment to be located may neither be used during the communication for purposes other than for its routing nor be retained or processed after the end of the communication without the consent of the subscriber**, who has been duly informed about the categories of data concerned, about the duration and purposes of the processing and about the fact that these data will or will not be passed on to third-party service providers". Furthermore, the subscriber will be able to withdraw or suspend his or her consent at any time and free of charge.

The draft Act states that data that may be retained in connection with the application of the proposed Articles 389-11-2 to 389-11-4 of the Criminal Code must relate exclusively to the identification of persons using the services supplied by the operators and service providers, to the technical characteristics of the communications provided by the latter and to the location of the terminal equipment. **They may on no account relate to the content of correspondence exchanged or information consulted**, in whatever form, in connection with these communications. Moreover, the retention and processing of data must comply with the provisions of the Protection of Personal Data Act of 23 December 1993, as amended[42] (proposed Article 389-11-5, first paragraph, of the Criminal Code).

Finally, the draft Act **imposes on operators and service providers the obligation to use their best endeavours to prevent uses of data other than those permitted** (proposed Article 389-11-5, para. 2, of the Criminal Code).

3. Procedural matters

The procedures to be implemented to block, filter and remove unlawful Internet depend on the fields concerned.

---

37 The draft Act defines "traffic data" as "all data relating to a communication by means of a computer system, generated by the latter as an element of the chain of communication, indicating the communication's origin, destination, route, time, date, size or duration or the type of underlying service" (Draft Act on combating technological crime of 24 February 2015, No. 934, page 24).

38 Draft Act on combating technological crime of 24 February 2015, No. 934, Section 2; draft of Article 389-11-2 *in limine* of the Criminal Code.

39 Ibid, draft of Article 389-11-3, paragraph 1, of the Criminal Code.

40 Ibid, paragraph 2.

41 Ibid, paragraph 3.

42 See points 2.1.2. and 2.2.2. of this report.

3.1. Protection of personal data

Section 3 of the Protection of Personal Data Act of 23 December 1993, as amended, provides: "**any natural or legal person whose rights […] have been infringed, or persons having reason to believe that such rights have been infringed**, may refer the matter to the President of the CCIN in order, if appropriate, to implement the measures [to verify that processing is carried out lawfully]". Moreover, Section 2(7) of the amended 1993 Act provides that the **CCIN may, on its own initiative**, verify the processing operation.

Sections 18 to 19 of the amended 1993 Act describe the **powers of the CCIN and the procedure to follow in cases of infringements of the obligations concerning the initiation and use of processing operations. These provisions have recently been modified**.

The former Section 18 of the amended 1993 Act described **CCIN's verification and investigation powers**. It provided that the CCIN could ensure the carrying out of the verifications and investigations necessary for checking the implementation of processing operations but provided **only few guarantees for those subjected to the CCIN's verifications**.

In the event of non-compliance with the procedural obligations relating to the initiation of a processing operation or in the event of a breach of the rules to be observed with regard to the use of data processing, the former section 19 of the amended 1993 Act provided: "the **President of the CCIN** shall send a **warning** to the person responsible or a **formal notice** to put an end to the irregularities or eliminate their effects. The irregularities that constitute criminal offences shall be immediately notified to the public prosecutor by the President of the CCIN. If the formal notice has not been acted upon after the expiry of the deadline, **the President of the Court of First Instance**, to which the President of the CCIN has referred the matter for an urgent ruling, shall order **all appropriate measures to put an end to the irregularities or eliminate their effects**, without prejudice to any criminal penalties incurred or to any demands for compensation made by data subjects who have suffered harm. The decision may be accompanied by a coercive fine. The previous provisions are not applicable to **legal entities established under public law**, in respect of which the President of the CCIN may require the Minister of State to take all necessary steps to put a stop to the irregularities established in order to ensure their effects are eliminated. With regard to services that do not fall within the remit of the Minister of State, the latter shall refer matters for the same reasons to the relevant administrative bodies and may, if the appropriate steps are not taken, act *proprio motu*".

However, the Supreme Court has, in three decisions dated 25 October 2013,[43] severely criticised the **unconstitutionality** of the former Section 18 in force at that time, since its provisions "violate the **principle of the inviolability of the home**, which is enshrined in Article 21 of Constitution, a violation that cannot be regarded as proportionate to the public interest aim pursued by the Act". This is because of "the scope of the investigative powers and the criminal penalties provided for […], in the absence [of appropriate guarantees]". In these decisions, the Supreme Court states that the framework laid down did not provide a sufficiently clear and precise guarantee of the rights of those

---

43 Supreme Court, 25.10.2013, S.A.M. Monaco Telecom International v. CCIN, available (in French only) at http://www.legimonaco.mc/305/legismc.nsf/06fbdeff618e11bec1257a4b003c5f29/ab1b56b85608432cc1257de4002f4ced!OpenDocument (accessed on 28 September 2015), S.A.M. Monaco Telecom v. CCIN, available (in French only) at http://www.legimonaco.mc/305/legismc.nsf/06fbdeff618e11bec1257a4b003c5f29/33bf2b73bb2b5506c1257de4002f4cf9!OpenDocument (accessed on 28 September 2015) and Sieur D. C. v. CCIN, available (in French only) at http://www.legimonaco.mc/305/legismc.nsf/06fbdeff618e11bec1257a4b003c5f29/d444bfa6dcc4c0b4c1257de4002f4d09!OpenDocument (accessed on 28 September 2015).

individuals and legal entities that process personal data and are subject to monitoring by the CCIN. **These decisions have resulted in rendering these provisions inoperative and, in practice, prevented the proper exercise of the CCIN's investigative and supervisory powers**. Accordingly, the Principality could have no longer been considered to provide an adequate level of personal data protection, especially by the European Commission, which is tasked with listing the European countries to which transfers of personal data are secure and therefore facilitated.[44]

In order to fill this legal vacuum, **the Act of 1st December 2015 amending Sections 18 and 19 of the amended Act of 23 December 1993 on the protection of personal data**[45] **(**hereinafter "the 2015 Act") has been adopted.

Among amendments to Section 18, of particular interest is the introduction of a provision designed to protect **medical confidentiality** by way of the exclusive intervention of a doctor to supervise processing operations containing medical personal data[46], a provision exempting persons subjected to **business secrets** from giving information to the CCIN while it exercises its supervisory powers,[47] an obligation to **jointly** draw up an **official report** when the supervision is on site or by summons[48] and the possibility for CCIN agents or investigators **to make findings based on their observations of web material**, thereby no longer requiring them to go on site to confirm the information found on the Internet.[49]

The 2015 Act also introduced a new Section 18-1 to the amended 1993 Act. It creates a **right** for the person responsible for the business or private premises or his/her representative **to oppose the CCIN supervision**. In the event of such opposition, the President of the CCIN has to call upon the President of the Court of First Instance. In order to make his/her decision, the latter takes into particular account the reasons for such opposition, or lack thereof. However, the right to oppose has an **exception: in cases of emergency or imminent risk of destruction or disappearance of evidence or a document**, it is not possible to oppose the supervisory operations. However, every interested person can apply to the President of the Court of First Instance to ask him/her to declare the supervisory operation as null and void, along with the evidential material collected, and to order its destruction.

The 2015 Act introduced one more Section to the amended 1993 Act: Section 18-2. This does not lay down a framework for the implementation of personal data processing, unlike the aforementioned Sections 18 and 18-1. It concerns **cases where "there exist reasons to suspect that the processing of**

---

44 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (accessed on 28 September 2015).

45 Act No. 1420 of 1st December 2015 amending Sections 18 and 19 of the Protection of Personal Data Act No. 1165 of 23 December 1993, available (in French only) at: http://www.conseil-national.mc/index.php/textes-et-lois/projets-de-loi/item/432-939-projet-de-loi-portant-modification-des-articles-18-et-19-de-la-loi-n-1165-du-23-decembre-1993-relative-a-la-protection-des-informations-nominatives.

46 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 18 paragraph 5.

47 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 18 paragraph 6.

48 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 18 last paragraph.

49 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 18 paragraph 7.

personal data does not conform to the provisions of [the amended 1993 Act]"[50]. In these cases, the President of the CCIN has to call upon the President of the Court of First Instance to obtain a **prior authorization** to access the premises concerned. The Court's order can be appealed, potentially leading to a decision to declare the supervisory operations and the evidence collected as null and void. This appeal has no suspensive effect, meaning that the decision remains applicable until a successful appeal.

The Act modifies Section 19 of the amended 1993 Act as well, introducing measures to guarantee respect of the **adversarial principle** where irregularities are observed, before the sending of the abovementioned warning and final demand,[51] and then a second time, before the aforementioned President of the Court of First Instance is seized.[52]

Indeed, the new Section 19 gives **one month for the person responsible for the processing of personal data to make comments after the report observing irregularities**, before the President of the CCIN can, alternatively or successively, provide a warning to the person responsible for treating the personal data who fails to respect his/her obligations under the amended 1993 Act, or send him/her a final demand to correct the irregularities or to remove their effects if he/she does not want to comply with these provisions. From now on, this procedure also affords protection to **legal entities established under public law**.

At the end of this procedure, Section 19 paragraph 4 provides that if the final demand does not have desired effect by the end of the period given to comply, **a new period of one month is given to the person responsible for the data processing in order for him/her to send his/her explanation to the President of the CCIN, failing which, the President will award an injunction** to end the processing operations or to remove its effects. If the injunction is not respected, the President of the CCIN can ask the Court of First Instance to order the termination of the data processing or the removal of its effects, possibly under the pain of a fine. Section 19 paragraph 4 is not applicable to legal entities established under public law, which remain under the Minister of State's authority and other competent administrative authorities, as already provided for under the former Section 19 before being amended by the 2015 Act.[53]

The amended Section 19 also contains a new **obligation for the President of the CCIN: to provide justification for his/her decisions** taken in applying this Section 19.[54]

The President of the CCIN can moreover decide **to publish his/her decisions** taken in applying Section 19, except where this would severely and disproportionately threaten public security, respect for private and family life or the legitimate interests of the persons concerned; in such cases, **the President of the Court of First Instance can order the withdrawal of the publication.**[55] Being a withdrawal and not a prohibition prior to publication, and in the absence of any measure designed to inform the persons concerned and the national authorities of the forthcoming publication, there is a concern that **severe and disproportionate infringements to public security, respect for private and**

---

50 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 18-2 paragraph 1.

51 See the quotation of the former Section 19 of the amended 1993 Act, above in paragraph 3.1 of this opinion.

52 *Ibidem.*

53 *Ibidem.*

54 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 19 paragraph 5.

55 Personal Data Protection Act, Act No. 1165 of 23 December 1993, as amended, Section 19 last paragraph.

family life or legitimate interests of the persons concerned will have already been perpetrated by the time that the judge makes a ruling, such damage being irreparable.

3.2. Punishment of crimes and offences against children

The Act of 26 December 2007 on harsher penalties for crimes and offences against children inserted into the Criminal Code Article 294-4, which lays down **an obligation for technical service providers to conduct operations to prevent public access to images of child pornography** and make these images available to the judicial authority.

Article 294-4 of the Criminal Code states that **this obligation comes into being as soon as technical service providers are made aware of images of child pornography**. No details are given about how this information is to be provided. In order to answer this question, it will probably be necessary to refer to the Digital Economy Act of 2 August 2011, in particular Section 29 (see point 2.2.1. of this report).

3.3. Draft Act on the electronic trade in medicines

The draft Act on the electronic trade in medicines and on group purchasing associations provides that the creation of an Internet site for sales of medicines shall require, in addition to its being attached to an existing pharmacy, the authorisation of the Minister of State issued after the submission of a reasoned opinion from the Council of the Order of Pharmacists. If the rules laid down are not complied with, the following procedure is set out in the draft: **the Minister of State will initially have to issue the pharmacist with a formal notice**, within a period of no less than eight days. In the event of failure to comply, **the Minister of State will be able to order the closure of the e-commerce site** for sales of medicines for a maximum period of five months. If during this closure the pharmacist has failed to comply with the rules applicable, **the Minister of State can revoke the above-mentioned authorisation**. **In an urgent case involving the safety of individuals or a danger to public health or the environment**, the site may be closed down temporarily without formal notice (Section 5 of the draft Act).

The draft Act contains no provision stipulating whether an authority will be tasked with carrying out the general monitoring of the online trade in medicines or a provision enabling an appeal to be lodged against a decision to close down an online pharmacy.

4. General monitoring of the Internet

4.1. Liability of technical service providers (Internet access providers and hosting providers)

Section 32.1 of the Digital Economy Act of 2 August 2011 provides that **technical service providers "shall not be subject to a general obligation to monitor the information [they] transmit or store, nor to a general obligation to search for facts or circumstances revealing unlawful activities"**.

Technical service providers may, however, be called upon to carry out from time to time any "targeted and temporary" monitoring operation **requested by the judicial authority**.

4.2. Special criminal investigation techniques in connection with correspondence sent by means of electronic communications

The "Justice and Freedom" Act of 26 December 2007 inserted into the Code of Criminal Procedure a number of provisions relating to special criminal investigation techniques relating to correspondence sent by means of electronic communications.[56] These techniques can be implemented to **establish the presence of unlawful Internet content** before possibly being subject to blocking, filtering or removal. These measures constitute general monitoring of the Internet only once a criminal investigation has been opened.

Article 106-1 of the Code of Criminal Procedure (hereinafter "the CCP") accordingly provides for the possibility for the **investigating judge** to order the interception, recording and transcription of correspondence sent by means of telecommunications or electronic communications in the case of a crime or misdemeanour punishable by one year's imprisonment or more.

The following article (Article 106-2 CCP) and Article 106-9 CCP adapt this provision to cases in which **business secrecy** must be protected.

Article 106-5, first paragraph, of the CCP provides: "**the investigating judge or police officer appointed by him/her may require any qualified employee of a network operator or a provider of telecommunications services or Internet access" "to install an interception device"**. The second paragraph of this article authorises them "to order any person with special knowledge of the telecommunications or electronic telecommunications system subject to the monitoring measure, including means of protecting and encrypting digital data, to provide information on the operation of that system and on how to access the content of data and communications in a comprehensible form".

Article 106-10 CCP provides for the **destruction of recordings and transcriptions once prosecution is barred under the statute of limitations**.

4.3. Draft Act on combating technological crime

Title III of the draft Act on combating technological crime provides for the **setting up of a specialised administrative authority to ensure the security of information systems**. This authority would be solely responsible for ensuring the security of the state information systems and sectors of activity of vital importance.[57] According to our research,[58] it will have the particular task of preventing, detecting and handling cyberattacks and controlling the security level of bodies of vital importance with the collaboration of the Direction of Electronic Communications[59] with regard to electronic

---

56 Code of Criminal Procedure, Articles 106-1 to 106-11.

57 Section 24, 2nd paragraph of draft Act No. 934 of 24 February 2015 on combating technological crime defines sectors of activity of vital importance as consisting of "activities with a common goal pertaining to the production and distribution of goods and services essential for meeting the basic needs of the Monegasque population, to the exercise of government authority, to the functioning of the economy and to state security".

58 An order creating this specialised administrative authority to ensure security of information systems should be taken soon.

59 The Direction of Electronic Communications is a Monegasque governmental entity, under the authority of the Government Counsellor for Public works, Environment and Urbanism. More information about the Direction of Electronic Communications is available at: http://en.gouv.mc/Government-Institutions/The-Government/Ministry-of-Public-Works-the-Environment-and-Urban-Development/Department-of-Electronic-Communications.

communications organisations and individuals operating the network or providing for telecommunication services or access to Internet. In order to achieve this, personal data processing, automatic or not, enabling identification of persons or goods, by any technical or computer-assisted means, could be implemented.

We have been unable to identify any police service specialising in **general Internet monitoring**, neither in terms of ex officio monitoring nor on the basis of offences being reported.

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

5.1. Liability of technical service providers (Internet access providers and hosting providers)

The Digital Economy Act of 2 August 2011, especially the Title relating to the liability of technical service providers, constitutes an **accessible legal basis**. It has been the subject of a publication.

The aim of the 2011 Act is to achieve the **legitimate goals pursued by the laws criminalising unlawful Internet activities**.

In this regard, the system for regulating the processing of personal data complies with the European Convention on Human Rights and the case law of its Court.

However, it is possible to question the extent to which it complies with the **legal foreseeability principle** and whether **sufficient protection is afforded against arbitrary action**.

As will have been seen from this report, **several activities considered unlawful outside the borders of the Principality, or which are indeed punishable under Monegasque legislation when not committed on the Internet, are not yet subject to provisions specific to their being carried out online** (for example, the online trade in medicines, the regulation of online gaming and protection of intellectual property on the Internet). It is therefore **difficult to ascertain whether technical service providers could be held liable** for breaches of the law committed through the Internet when their actions are unlawful only outside the Internet or beyond the Principality's borders.

The adequacy of the protection afforded against arbitrary action by a technical service provider's decision to block, filter or remove content notified to it as unlawful could also be questioned. If they do not want to be held civilly or criminally liable, technical service providers should in fact remove or block content notified to them as unlawful by anyone. The 2011 Act does not impose any restrictions regarding persons who can make such a notification and **does not provide for prior judicial scrutiny of the actual nature of the unlawfulness**. The only limit imposed consists of penalties for deliberately inaccurate reports. Such practices may well lead to a tendency for technical service providers to go too far in blocking or removing Internet content (chilling effect), without giving sufficient consideration to freedom of expression.

5.2. Protection of personal data

The Protection of Personal Data Act of 23 December 1993, as amended, constitutes an **accessible and foreseeable legal basis**. It has been the subject of a publication. Its content is easy to understand and it is also communicated to the public in several practical guides for professionals and private individuals.

The 1993 Act, as amended, pursues the **legitimate aim of guaranteeing the protection of the rights of others**.

In this regard, the system for regulating the processing of personal data **complies** with the European Convention on Human Rights and the case law of its Court.

However, in 2013, a Monegasque court has had occasion to observe[60] that the **investigative and supervisory powers of the CCIN**, as defined at that time, **violated "the principle of the inviolability of the home […], a violation that cannot be regarded as proportionate to the public interest aim pursued by the Act".** This is because of "the scope of the investigative powers and the criminal penalties provided for […], in the absence [of proper guarantees]".

Furthermore, the above-mentioned decisions have resulted in the **de facto paralysis of the investigative and supervisory powers of the CCIN**, until adoption of the 2015 Act amending the provisions denounced by the Monegasque court. This could have had as a consequence the conclusion that the Principality was failing to honour its international commitments since the CCIN would in practice not be implementing the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Therefore, the amended 1993 Act **did not comply** with the European Convention on Human Rights and the case law of its Court. Nevertheless, **the 2015 Act corrects these infringements, going forwards, thereby enabling Monegasque Law to comply** with the European Convention of Human Rights and the case law of its Court.

5.3. Punishment of crimes and offences against children

An examination of the Act of 26 December 2007 on harsher penalties for crimes and offences against children can be divided into two parts.

The provisions making actions against children via the Internet criminal offences or the imposition of harsher penalties seem to be in compliance with the European Convention on Human Rights and the Court's case law as this is an accessible and foreseeable law that pursues a legitimate aim and imposes the restrictions necessary in a democratic society.

However, just as in the case of the 2011 Digital Economy Act, the question may be raised as to whether **sufficient protection is afforded against arbitrary action**, since technical service providers must block or remove content notified to them as unlawful without any prior judicial scrutiny (Article 294-4 of the Criminal Code).

However, with regard to the punishment of crimes and offences against children, the absence of judicial scrutiny is **justified by the seriousness and urgency of the suspected acts**.

5.4. Special criminal investigation techniques in connection with correspondence sent by means of electronic communications

The "Justice and Freedom" Act of 26 December 2007 lays down the **criminal procedure to be followed to establish the presence of unlawful content in correspondence** sent by means of electronic communications.

---

60 Supreme Court, 25 October 2013, S.A.M. Monaco Telecom International v. CCIN, S.A.M. Monaco Telecom v. CCIN, and Sieur D. C. v. CCIN. Decisions cited in Section 3.1. of this report.

This Act may be considered to be **in compliance with the requirements** of the European Convention on Human Rights and the Court's case law since the **provisions described are accessible and foreseeable; the involvement of the investigating judge** ensures sufficient protection **against** arbitrary action and the abuse of law; several **legitimate aims** can be established (the legitimate aim will depend on the breach of the law concerned, for example a breach of national security or the prevention of disorder); and the interference with correspondence may be considered proportionate because, firstly, the court orders interception, recording or transcription **only in the case of a crime or misdemeanour punishable by one year's imprisonment or more**, secondly, **business secrecy** is protected by the relevant provisions and, thirdly, recordings and transcriptions are **destroyed once prosecution is barred under the statute of limitations**.

Carole Viennet
Legal Adviser, Swiss Institute of Comparative Law

Stéphanie De Dycker, LL.M.
Legal Adviser, Swiss Institute of Comparative Law

10.12.2015

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