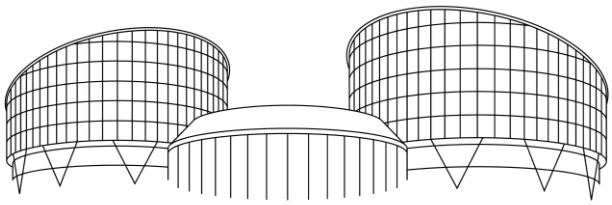

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

SECOND SECTION

CASE OF AHMET YILDIRIM v. TURKEY

(Application no. 3111/10)

JUDGMENT

STRASBOURG

18 December 2012

FINAL

18/03/2013

This judgment has become final under Article 44 § 2 of the Convention.

In the case of Ahmet Yıldırım v. Turkey,

The European Court of Human Rights (Second Section), sitting as a Chamber composed of:

Guido Raimondi, *President*,
Danutė Jočienė,
Dragoljub Popović,
András Sajó,
Işıl Karakaş,
Paulo Pinto de Albuquerque,
Helen Keller, *judges*,
and Stanley Naismith, *Section Registrar*,

Having deliberated in private on 20 November 2012,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 3111/10) against the Republic of Turkey lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Turkish national, Mr Ahmet Yıldırım ("the applicant"), on 12 January 2010.

2. The applicant was represented by Ms A. Kaymak, a lawyer practising in İzmir. The Turkish Government ("the Government") were represented by their Agent.

3. The applicant alleged, in particular, that the blocking of access to his Internet site, ordered by the national authorities, amounted to an unjustified infringement of his rights under Articles 6, 7, 10 and 13 of the Convention and Article 2 of Protocol No. 1.

4. On 31 January 2011 notice of the application was given to the Government. It was also decided to rule on the admissibility and merits of the application at the same time (Article 29 § 1 of the Convention).

5. The applicant filed further observations (Rule 59 § 1 of the Rules of Court). Third-party comments were also received from the association Open Society Justice Initiative, which had been given leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 2).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

6. The applicant was born in 1983 and lives in Istanbul.

7. The applicant owns and runs a website (http://sites.google.com/a/ahmetyildirim.com.tr/academic/) on which he publishes his academic work and his views on various topics. The website was created using the Google Sites website creation and hosting service (http://sites.google.com/).

8. On 23 June 2009, under section 8(1)(b) of Law no. 5651 on regulating Internet publications and combating Internet offences, the Denizli Criminal Court of First Instance ordered the blocking of the website http://sites.google.com/site/kemalizminkarinagrisi/benimhikayem/atatuerk-koessi/at (hereinafter "the offending website"). The order was issued as a preventive measure in the context of criminal proceedings against the site's owner, who was accused of insulting the memory of Atatürk.

9. On the same day, under section 8(3) of Law no. 5651, a copy of the blocking order was sent to the Telecommunications and Information Technology Directorate ("the TİB") for execution.

10. On 24 June 2009, at the request of the TİB, the Denizli Criminal Court of First Instance varied its decision of 23 June and ordered the blocking of all access to Google Sites under section 8 of Law no. 5651. The TİB had indicated that this was the only means of blocking the offending website, as its owner did not have a server certificate and lived abroad.

11. The TİB, implementing the order of 24 June 2009, blocked all access to Google Sites and the applicant was thus unable to access his own website. All his subsequent attempts to remedy the situation were unsuccessful because of the blocking order issued by the court.

12. On 1 July 2009 the applicant applied to have the blocking order of 24 June 2009 set aside in respect of his website. He pointed out that he used the website regularly in order to publish his academic work and his opinions on various topics, and that the measure had barred all access to his site, which had no connection with the offending website. He argued, in particular, that in order to prevent other websites being affected by the measure, a method should have been chosen which would make only the offending website inaccessible. He cited as an example blocking the site's URL.

In support of his request, the applicant furnished the court with a copy of the webpage which appeared when he tried to access his own website. The following warning was displayed:

> "The Telecommunications and Information Technology Directorate has applied the order issued by the Denizli Criminal Court of First Instance on 24 June 2009 in respect of this website (sites.google.com) as a preventive measure."

13. On 13 July 2009 the Denizli Criminal Court dismissed the applicant's application. Referring to a recommendation issued by the TİB, it considered that the only means of blocking access to the offending website, in accordance with the blocking order, had been to block access to the Google Sites service, which had hosted the content complained of.

14. The applicant wrote to the Court on 25 April 2012 informing it that he was still unable to access his website even though, as far as he understood it, the criminal proceedings against the owner of the offending website had been discontinued on 25 March 2011 because of the impossibility of determining the identity and address of the accused, who lived abroad.

II. RELEVANT DOMESTIC LAW

Law no. 5651 of 4 May 2007 on regulating Internet publications and combating Internet offences

15. The relevant parts of Law no. 5651 read as follows:

Section 2
Definitions

"(1) For the purposes of this Law,

...

(e) Access provider [(*erişim sağlayıcı*) shall mean] any natural or legal person which provides users with Internet access;

(f) Content provider [(*içerik sağlayıcı*) shall mean] any natural or legal person which produces, modifies or supplies any kind of information or data for Internet users;

...

(ğ) Internet publication [(*yayın*) shall mean] data which can be accessed via the Internet by an indeterminate number of persons;

...

(l) Publication [(*yayın*) shall mean] publication on the Internet;

..."

Section 4
Liability of content providers

"(1) Content providers shall be held liable for any content they provide via the Internet.

(2) Content providers shall not be held liable for content belonging to others which can be accessed by means of a link provided by them ...

..."

Section 5
Liability of hosting service providers

"(1) Hosting service providers shall not be required to monitor the content hosted by them or to ascertain whether it constitutes illegal activity.

(2) Subject to their criminal responsibility, hosting service providers who are informed, in accordance with sections 8 and 9 of this Law, of the illegal nature of content hosted by them shall be required to cease publishing it, in so far as they have the technical capacity to do so."

Section 6
Liability of access providers

"(1)(a) Where they are informed, in accordance with the provisions of this Law, of the illegal nature of content published by a user, access providers shall be required to block access to the illegal content, in so far as they have the technical capacity to do so.

...

(2) Access providers shall not be required to monitor the legality of the content and information to which they provide access.

..."

Section 8
Blocking orders and implementation thereof

"(1) A blocking order [*erişimin engellenmesi*] shall be issued in respect of Internet publications where there are sufficient grounds to suspect that their content is such as to amount to one of the following offences:

(a) offences under the Criminal Code ...

(1) incitement to suicide (Article 84);

(2) sexual abuse of minors (Article 103 § 1);

(3) facilitating the use of narcotic drugs (Article 190);

(4) supplying products dangerous to health (Article 194);

(5) obscenity (Article 226);

(6) prostitution (Article 227);

(7) hosting gambling activities;

(b) offences against Atatürk under Law no. 5816 of 25 July 1951;

...

(2) The blocking order shall be issued by a judge if the case is at the investigation stage or by the court if a prosecution has been brought. During the investigation, the blocking of access may be ordered by the public prosecutor in cases where a delay in acting could have harmful effects. The order must then be submitted to the judge for approval within twenty-four hours. The judge must give a decision within a further twenty-four hours. If he or she does not approve the blocking of access, the measure shall be lifted by the prosecutor forthwith. Blocking orders issued as a preventive

measure may be appealed against in accordance with the provisions of the Code of Criminal Procedure (Law no. 5271).

(3) A copy of the blocking order issued by the judge, court or public prosecutor shall be sent to the [Telecommunications and Information Technology] Directorate for execution.

(4) Where the content provider or the hosting service provider is abroad ... the blocking order shall be issued by the Directorate of its own motion. It shall then be notified to the access provider with a request for execution.

(5) Blocking orders shall be implemented immediately or at the latest twenty-four hours after notification.

...

(7) If the criminal investigation ends in a decision to discontinue the proceedings, the blocking order shall automatically cease to apply ...

(8) Where the trial ends in an acquittal, the blocking order shall automatically cease to apply ...

(9) If the illegal content is removed, the blocking order shall be lifted ..."

16. The Telecommunications and Information Technology Directorate was established under provisional section 7 of Law no. 2559 on police powers and responsibilities, as amended on 3 July 2005 by Law no. 5397. As an administrative body it is responsible, among other tasks, for recording and monitoring information disseminated using telecommunications tools.

17. In practice, where a court orders the blocking of access to a specific website, it falls to the TİB to implement the measure. If the content provider or hosting service provider is abroad, the TİB may block all access to the pages of the intermediary service provider under section 8(3) and (4) of Law no. 5651. Therefore, the issuing of a blocking order does not result only in access to the website which is the subject of criminal proceedings being blocked; access to all the content on the Internet domain concerned is also liable to be blocked. Thus, domains such as blogspot.com, blogger.com, Google Groups, myspace.com and youtube.com have been the subject of blocking orders over long periods of time because of the websites which they host.

18. The notion of what constitutes a "publication" within the meaning of section 2(1) of Law no. 5651 has also been the subject of debate among legal commentators. In the view of some commentators, sub-paragraph (ğ), according to which the concept of "Internet publication" denotes "data which can be accessed via the Internet by an indeterminate number of persons" is in contradiction with the notion contained in subsection (l) of the same section, which states that "[p]ublication [(*yayın*) shall mean] publication on the Internet". The difficulty stems from the reference to "data which can be accessed via the Internet", which could apply to all kinds of data transmitted over the Internet.

III. INTERNATIONAL LAW AND PRACTICE

A. Council of Europe

1. Convention on Cybercrime

19. The Convention on Cybercrime (ETS No. 185), which came into force on 1 July 2004, was drawn up by the member States of the Council of Europe, Canada, Japan, South Africa and the United States of America. It deals with various types of offences in the sphere of cybercrime: action directed against the confidentiality, integrity and availability of computer data and systems; computer-related forgery and fraud; content-related offences, especially those related to child pornography; and offences concerning infringements of copyright and related rights (Chapter II, Section 1, Titles 1-4).

2. Committee of Ministers

(a) Declaration CM(2005)56 final

20. The preamble to the Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final of 13 May 2005) recognises that "limited or no access to [information and communication technologies (ICTs)] can deprive individuals of the ability to exercise fully their human rights". The first chapter of the Declaration, entitled "Human rights in the Information Society" contains the following passages:

> "**1. The right to freedom of expression, information and communication**
>
> ICTs provide unprecedented opportunities for all to enjoy freedom of expression. However, ICTs also pose many serious challenges to that freedom, such as State and private censorship.
>
> Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the [Convention], simply because communication is carried in digital form.
>
> In guaranteeing freedom of expression, member States should ensure that national legislation to combat illegal content, for example racism, racial discrimination and child pornography, applies equally to offences committed via ICTs.
>
> Member States should maintain and enhance legal and practical measures to prevent State and private censorship. ..."

(b) Declaration of 28 May 2003

21. The preamble to the Declaration on freedom of communication on the Internet adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies states that prior control of

communications on the Internet, regardless of frontiers, should remain an exception, and that there is a need to remove barriers to individual access to the Internet. The Declaration sets forth, *inter alia*, the following principles:

> "...
>
> Principle 1: Content rules for the Internet
>
> Member States should not subject content on the Internet to restrictions which go further than those applied to other means of content delivery.
>
> ...
>
> Principle 3: Absence of prior State control
>
> Public authorities should not, through general blocking or filtering measures, deny access by the public to information and other communication on the Internet, regardless of frontiers. This does not prevent the installation of filters for the protection of minors, in particular in places accessible to them, such as schools or libraries.
>
> Provided that the safeguards of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms are respected, measures may be taken to enforce the removal of clearly identifiable Internet content or, alternatively, the blockage of access to it, if the competent national authorities have taken a provisional or final decision on its illegality.
>
> ..."

22. The explanatory note to the Declaration includes the following commentary on Principle 3:

> "Absence of prior State control
>
> This principle underlines the importance of no prior State control over what the public can search for on the Internet. In some countries, there is a tendency to block access by the population to content on certain foreign or domestic websites for political reasons. This and similar practices of prior State control should be strongly condemned.
>
> Although the State should by no means take broad measures to block undesirable content, exceptions must be allowed for the protection of minors. Where minors have access to the Internet, for example in schools or libraries, public authorities may require filters to be installed on computers to block access to harmful content.
>
> The absence of prior control by the State does not of course rule out measures being undertaken to remove content from the Internet or block access to it following a preliminary or final decision of the competent national authorities on its illegality, not only under penal law, but also under other branches of law such as civil or administrative law. This would typically be the case when injunctions are sought to prevent the publication on the Internet of content which is illegal. Such measures, which could entail some sort of prior control, would have to fulfil the requirements of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms and they would have to be directed at a clearly identifiable Internet content."

(c) Recommendation CM/Rec(2007)16

23. In 2007 the Committee of Ministers adopted Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet. The second and third chapters, entitled "Access" and "Openness" respectively, deal implicitly with the issues of accessibility of the Internet and the restrictions that may be permitted.

(d) Recommendation CM/Rec(2007)11

24. Also in 2007, the Committee of Ministers adopted Recommendation CM/Rec(2007)11 on promoting freedom of expression and information in the new information and communications environment.

(e) Recommendation CM/Rec(2008)6

25. In 2008 the Committee of Ministers adopted Recommendation CM/Rec(2008)6. The appendix to this Recommendation sets out guidelines on using and controlling Internet filters in order to fully exercise and enjoy the right to freedom of expression and information.

(f) Recommendation CM/Rec(2012)3

26. On 4 April 2012 the Committee of Ministers adopted Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines. Paragraph 1 of the Recommendation stresses, *inter alia*, that "[s]earch engines enable a worldwide public to seek, receive and impart information and ideas and other content in particular to acquire knowledge, engage in debate and participate in democratic processes".

B. European Union

(a) Recommendation 2008/2160(INI)

27. Recommendation 2008/2160(INI), adopted by the European Parliament on 26 March 2009, stated expressly that States should participate in efforts to establish an e-democracy on the basis of full and safe access to the Internet. Parliament therefore recommended to member States that they should condemn government-imposed censorship of the content that could be searched on Internet sites, and called on them "to ensure that freedom of expression is not subject to arbitrary restrictions from the public and/or private sphere and to avoid all legislative or administrative measures that could have a 'chilling effect' on all aspects of freedom of speech".

(b) Case of *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (Court of Justice of the European Union)

28. Case C-70/10, examined by the Court of Justice of the European Union (CJEU), concerned a reference for a preliminary ruling following an

order issued by a Belgian court requiring an Internet service provider to install a permanent monitoring system blocking all online activity liable to infringe intellectual property rights.

29. In its judgment of 24 November 2011 the CJEU held that the holders of intellectual property rights should have the possibility of applying for an injunction against an intermediary who carried a third party's infringement of a protected work or other subject matter in a network, and that the arrangements governing such injunctions should be left to national law. However, the national rules had to observe the limitations arising from European Union law and in particular from the Directive on electronic commerce (2000/31/EC), which prohibited national authorities from adopting measures which would require an Internet service provider to carry out general monitoring of the information that it transmitted on its network. The CJEU took the view that injunctions of the kind issued in the case under consideration did not respect the requirement that a fair balance be struck between the right to intellectual property on the one hand and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information on the other. Accordingly, it concluded that European Union law, and in particular Directive 2000/31/EC and the applicable fundamental rights, precluded an injunction imposed on an Internet service provider to introduce a system for filtering all electronic communications passing via its services, applied indiscriminately to all its customers, as a preventive measure, exclusively at its expense and for an unlimited period.

C. United Nations Human Rights Committee

30. In its General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights, adopted at its 102nd session (11-29 July 2011), the United Nations Human Rights Committee stated as follows:

> "43. Any restrictions on the operation of websites, blogs or any other Internet-based, electronic or other such information-dissemination system, including systems to support such communication, such as Internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information-dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government."

IV. COMPARATIVE LAW

31. In view of the fact that legislation concerning the Internet, which has to be seen against a background of rapidly changing new technologies, is

particularly dynamic and fragmented, it is difficult to identify common standards based on a comparison of the legal situation in Council of Europe member States. A survey carried out by the Court of the legislation of twenty member States (Austria, Azerbaijan, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Ireland, Italy, Lithuania, the Netherlands, Poland, Portugal, Romania, Russia, Slovenia, Spain, Switzerland and the United Kingdom) reveals that the right to Internet access is protected in theory by the constitutional guarantees applicable to freedom of expression and freedom to receive ideas and information. The right to Internet access is considered to be inherent in the right to access information and communication protected by national Constitutions, and encompasses the right for each individual to participate in the information society and the obligation for States to guarantee access to the Internet for their citizens. It can therefore be inferred from all the general guarantees protecting freedom of expression that a right to unhindered Internet access should also be recognised.

32. In a decision of 10 June 2009 (no. 2009-58 DC), the French Constitutional Council, for instance, stated clearly that freedom of expression implied freedom of access to the Internet. The Constitutional Council also set forth a number of basic principles concerning the restriction of Internet access. Restrictions on the public's right to access online communication services could be ordered only by a judge, following a fair trial, and had to be proportionate. Finding that "in view of the nature of the freedom guaranteed by Article 11 of the 1789 Declaration, the legislature may not ... confer powers [to restrict or prevent Internet access] on an administrative authority with the aim of protecting the holders of copyright and related rights", the Constitutional Council declared to be unconstitutional the legislative provisions which provided for the blocking of Internet access in cases of infringement of copyright, in the absence of a prior judicial decision. It held that the suspension of access could be ordered only after adversarial judicial proceedings, as an ancillary penalty. Interim measures or injunctions could be ordered by the urgent-applications judge, provided that they were "strictly necessary in order to preserve the rights in question".

33. As regards possible restrictions in cases of illegal Internet content, European countries have adopted a wide variety of approaches and legislative measures, ranging from the suspension of individual rights of Internet access or the removal of the illegal content, to the blocking of access to the specific website in question. In most European countries, the protection of the rights of minors and efforts to combat the sexual exploitation of minors constitute a basis for appropriate measures restricting access to the websites concerned (this is the case in France, Germany, Switzerland and the United Kingdom). When it comes to ordinary crime,

the measures restricting access are different and less severe in six countries (Austria, Estonia, Finland, Italy, Lithuania and the Netherlands).

34. As to the scope of the restrictions, a distinction is generally made according to the nature of the offence committed, namely between offences against intellectual property rights and other offences. According to a report by the Organization for Security and Co-operation in Europe (OSCE) entitled "Freedom of expression on the Internet: study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States", there are no general legislative provisions on the blocking of Internet access in Austria, the Czech Republic, Germany or Poland. Five countries (Estonia, Finland, the Netherlands, Russia and the United Kingdom) have no legislation providing for wholesale blocking irrespective of the offence but have enacted specific legislative provisions allowing access to be blocked in the case of certain types of offence. These include child pornography, racism, hate speech, incitement to terrorism and defamation.

35. In Russia, although a blanket prohibition on Internet access is not possible, access restrictions may be imposed under federal legislation on specific grounds, for instance to protect the foundations of the constitutional order, morals, health or the legitimate rights and interests of others, or in the interests of national defence and security (Federal Law no. 149-FZ).

36. In those countries which do not have a general or specific legislative framework providing for the closure of sites and/or the blocking of access, blocking measures may nonetheless be ordered by a judge or applied on a voluntary basis.

37. The possibility of appealing against a measure prohibiting Internet access is closely linked to the general guarantees protecting the right to receive information and to express one's views. In Azerbaijan, Belgium, the Czech Republic, Lithuania, Spain and the United Kingdom, no specific provisions exist governing appeals against measures restricting access to an Internet page. Reference is made instead to the general constitutional provisions on freedom of expression and information or, in the case of the United Kingdom, to the possibility of judicial review if the user can prove that he or she has a sufficient interest linked to the subject of the impugned measure. In Estonia, the legislation makes express provision for contesting a measure restricting access to information on the Internet before a higher administrative authority or a specialised agency or directly before the courts in cases concerning public information which the authorities are required to make accessible (the Public Information Act).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 10 OF THE CONVENTION

38. The applicant complained of the impossibility of accessing his Internet site as a result of a measure ordered in the context of criminal proceedings which were wholly unrelated to his site. In his view, the measure amounted to an infringement of his freedom to receive and impart information and ideas, guaranteed by Article 10 of the Convention, which reads as follows:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

39. The Government did not submit any observations.

A. Admissibility

40. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

41. The applicant submitted that the blocking of Google Sites amounted to indirect censorship. He contended that the consequences that had resulted for him from the blocking order, namely his inability to access his own website, although the latter had no connection with the illegal content that had given rise to the blocking order in respect of Google Sites, had been disproportionate to the objectives pursued. He further maintained that the proceedings leading to the blocking of Google Sites could not be regarded as fair and impartial.

42. The Government did not submit any observations.

2. Third-party intervener

43. Referring to the Court's case-law, the association Open Society Justice Initiative observed that, since Google Sites hosted a large quantity of data and information and was thus comparable to the online archives of major newspapers or traditional libraries, the impugned measure amounted to a prior restraint on publication. Whereas the aim of the measure taken in this case had been to block access to a single website which was disseminating content insulting the reputation of Atatürk, access to the whole of Google Sites, which hosted the offending website, had been blocked. A measure of that nature, blocking access to such a quantity of information for an indeterminate period, was analogous to prior restraint as it prevented Internet users from accessing the blocked content for an indeterminate period. Such restrictions posed significant dangers and therefore required the most careful scrutiny by the Court.

44. Open Society Justice Initiative added that blocking orders which prevented access to a group of websites posed a risk of "collateral censorship". Such measures should therefore be avoided as being disproportionate where it was technically possible to target only the offending website. Citing examples from member States of the Council of Europe, the association observed that no large-scale blocking of Internet content comparable to that ordered in the present case had ever been ordered in France, Germany or the United Kingdom.

45. Furthermore, the Turkish system did not afford adequate safeguards against arbitrariness; for instance, there was no requirement to notify content providers or owners of other sites affected by the blocking order. In addition, numerous blocking orders had been issued in respect of websites which had thousands of users without any safeguards being applied. Access to sites including youtube.com, GeoCities and Dailymotion and to numerous Google services had been blocked over periods of months or even years, causing considerable "collateral censorship".

3. The Court's assessment

(a) Whether there was interference

46. The Court observes that the applicant owns and runs a website which he apparently uses in order to publish his academic work and his views on various topics. He complained of his inability to access his website as a result of a measure ordered in the context of criminal proceedings which were unconnected to his site. This amounted in his view to a prior restraint, imposed before a ruling had been given on the merits.

47. The Court reiterates that Article 10 does not prohibit prior restraints on publication as such. This is borne out not only by the words "conditions", "restrictions", "preventing" and "prevention" which appear in that provision, but also by the Court's judgment in The Sunday Times *v. the*

United Kingdom (no. 1) (26 April 1979, Series A no. 30) and in *markt intern Verlag GmbH and Klaus Beermann v. Germany* (20 November 1989, Series A no. 165). On the other hand, the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court. This is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest. This danger also applies to publications other than periodicals that deal with a topical issue.

48. As regards the importance of Internet sites in the exercise of freedom of expression, the Court reiterates that, in *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)* (nos. 3002/03 and 23676/03, § 27, ECHR 2009), it found as follows:

> "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general."

49. These considerations are also valid in the present case. The Court notes that Google Sites is a Google service designed to facilitate the creation and sharing of websites within a group and thus constitutes a means of exercising freedom of expression.

50. In that regard it points out that Article 10 guarantees freedom of expression to "everyone". It makes no distinction according to the nature of the aim pursued or the role played by natural or legal persons in the exercise of that freedom (see *Çetin and Others v. Turkey*, nos. 40153/98 and 40160/98, § 57, ECHR 2003-III). It applies not only to the content of information but also to the means of dissemination, since any restriction imposed on the latter necessarily interferes with the right to receive and impart information (see, *mutatis mutandis*, *Autronic AG v. Switzerland*, 22 May 1990, § 47, Series A no. 178). Likewise, the Court has consistently emphasised that Article 10 guarantees not only the right to impart information but also the right of the public to receive it (see Observer *and* Guardian *v. the United Kingdom*, 26 November 1991, § 59 (b), Series A no. 216, and *Guerra and Others v. Italy*, 19 February 1998, § 53, *Reports of Judgments and Decisions* 1998-I).

51. In the present case the measure blocking access to the website stemmed from a decision of the Denizli Criminal Court of First Instance. It was initially designed as a preventive measure ordered by the court in the context of the criminal proceedings brought against a third-party website under Law no. 5816 prohibiting insults against the memory of Atatürk. However, the administrative body responsible for executing the blocking order, the TİB, requested that an order be given blocking all access to Google Sites. In a decision of 24 June 2009, the Denizli Criminal Court of First Instance granted the request. Ruling on an application by the applicant to have it set aside, the Denizli Criminal Court subsequently upheld the order, taking the view that the only means of blocking access to the website

that was the subject of criminal proceedings was to block access to Google Sites. The TİB therefore blocked access to the entire Google Sites domain, thereby incidentally preventing the applicant from accessing his own website. It appears from the case file that, as a result of the measure, the applicant was completely unable for an indeterminate period of time to access his own website. All his attempts to do so were unsuccessful because of the blocking order issued by the court. He can therefore legitimately claim that the measure in question affected his right to receive and impart information and ideas.

52. The crux of the case therefore concerns the collateral effect of a preventive measure adopted in the context of judicial proceedings. Although neither Google Sites as such nor the applicant's website was the subject of the proceedings in question, the TİB blocked access to them in order to execute the measure ordered by the Denizli Criminal Court of First Instance. The measure was to remain in place until such time as a decision was given on the merits or the illegal content of the site hosted by Google Sites was removed (section 9 of Law no. 5651). It therefore constituted a prior restraint as it was imposed before a ruling had been given on the merits.

53. The Court considers that, whatever its legal basis, such a measure was bound to have an influence on the accessibility of the Internet and, accordingly, engaged the responsibility of the respondent State under Article 10 (see, *mutatis mutandis*, *Vereinigung demokratischer Soldaten Österreichs and Gubi v. Austria*, 19 December 1994, § 27, Series A no. 302).

54. It further observes that the blocking of access complained of resulted from a prohibition initially imposed on a third-party website. It was the blocking of all access to Google Sites which actually affected the applicant, who owned another website hosted on the same domain. It is true that the measure did not, strictly speaking, constitute a wholesale ban but rather a restriction on Internet access which had the effect of also blocking access to the applicant's website. Nevertheless, the fact that the effects of the restriction in issue were limited does not diminish its significance, especially since the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest.

55. In sum, the Court considers that the impugned measure amounted to a restriction stemming from a preventive order blocking access to an Internet site. For the purpose of executing the latter, the Denizli Criminal Court of First Instance further ordered, at the request of the TİB, the blocking of access to Google Sites, which also hosted the applicant's website. The applicant was thereby prevented from accessing his own website. This circumstance is sufficient for the Court to conclude that the measure in question amounted to "interference by public authority" with the

applicant's right to freedom of expression, of which the freedom to receive and impart information and ideas is an integral part (see, *mutatis mutandis*, *Ayşe Öztürk v. Turkey*, no. 24914/94, § 58, 15 October 2002).

56. Such interference will constitute a breach of Article 10 unless it is "prescribed by law", pursues one or more of the legitimate aims referred to in Article 10 § 2 and is "necessary in a democratic society" to achieve those aims.

(b) Prescribed by law

57. The Court reiterates at the outset that the expression "prescribed by law", within the meaning of Article 10 § 2, requires firstly that the impugned measure should have some basis in domestic law; however, it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences, and that it should be compatible with the rule of law (see, among many other authorities, *Dink v. Turkey*, nos. 2668/07, 6102/08, 30079/08, 7072/09 and 7124/09, § 114, 14 September 2010). According to the Court's established case-law, a rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct (see, among many other authorities, *RTBF v. Belgium*, no. 50084/06, § 103, ECHR 2011, and *Altuğ Taner Akçam v. Turkey*, no. 27520/07, § 87, 25 October 2011).

58. In the instant case the Court observes that the blocking of access to the website which was the subject of judicial proceedings had a statutory basis, namely section 8(1) of Law no. 5651. As to whether this section also satisfied the requirements of accessibility and foreseeability, the applicant submitted that this question should be answered in the negative, as the provision in question was too uncertain in his view.

59. The Court has consistently held that, for domestic law to meet these requirements, it must afford a measure of legal protection against arbitrary interferences by public authorities with the rights guaranteed by the Convention. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion and the manner of its exercise (see, among many other authorities, The Sunday Times, cited above, § 49, and *Maestri v. Italy* [GC], no. 39748/98, § 30, ECHR 2004-I).

60. The question here is whether, at the time the blocking order was issued, a clear and precise rule existed enabling the applicant to regulate his conduct in the matter.

61. The Court observes that, under section 8(1) of Law no. 5651, a judge may order the blocking of access to "Internet publications where there are

sufficient grounds to suspect that their content is such as to amount to ... offences". Section 2 of the same Law provides two definitions of the notion of "publication": according to sub-paragraph (ğ) "Internet publication [(*yayın*) shall mean] data which can be accessed via the Internet by an indeterminate number of persons". Subsection (l), meanwhile, states that "[p]ublication [(*yayın*) shall mean] publication on the Internet". Even though the notion of "publication" appears to be very broad and may cover all kinds of data published on the Internet, it is clear that neither the applicant's website nor Google Sites *per se* fell within the scope of section 8(1) of Law no. 5651, since the legality of their content, within the meaning of that provision, was not in issue in the present case.

62. Neither Google Sites nor the applicant's website was the subject of judicial proceedings for the purposes of section 8(1) of Law no. 5651. It is clear from the fact that this provision was referred to in the decision of 24 June 2009 (see paragraph 10 above) that Google Sites was held to be liable for the content of a website which it hosted. However, sections 4, 5 and 6 of Law no. 5651, which deal with the liability of content providers, hosting service providers and access providers, make no provision for a wholesale blocking of access such as that ordered in the present case. Nor has it been maintained that the Law authorised the blocking of an entire Internet domain like Google Sites which allows the exchange of ideas and information. Moreover, there is nothing in the case file to indicate that Google Sites was notified under section 5(2) of Law no. 5651 that it was hosting illegal content, or that it refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings.

63. The Court also observes that section 8, subsections (3) and (4), of Law no. 5651 conferred extensive powers on an administrative body (the TİB) in the implementation of a blocking order originally issued in relation to a specified site. The facts of the case demonstrate that the TİB could request the extension of the scope of a blocking order even though no proceedings had been brought against the website or domain in question and no real need for wholesale blocking had been established.

64. As indicated above (see paragraph 47), the Court considers that such prior restraints are not necessarily incompatible with the Convention as a matter of principle. However, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power (see *Association Ekin v. France*, no. 39288/98, § 58, ECHR 2001-VIII, and, *mutatis mutandis*, *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05, § 55, ECHR 2011). In that regard, the judicial review of such a measure, based on a weighing-up of the competing interests at stake and designed to strike a balance between them, is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression (see *RTBF v. Belgium*, cited above, § 114). The Court observes

that when the Denizli Criminal Court of First Instance decided to block all access to Google Sites under Law no. 5651 it merely referred to a recommendation from the TİB, without ascertaining whether a less far-reaching measure could have been taken to block access specifically to the offending website (see paragraph 10 above).

65. The Court also notes that in his application of 1 July 2009 to have the blocking order set aside one of the applicant's main arguments was that, to prevent other websites from being affected by the measure in question, a method should have been chosen whereby only the offending website was made inaccessible.

66. However, there is no indication that the judges considering the application sought to weigh up the various interests at stake, in particular by assessing the need to block all access to Google Sites. In the Court's view, this shortcoming was simply a consequence of the wording of section 8 of Law no. 5651 itself, which did not lay down any obligation for the domestic courts to examine whether the wholesale blocking of Google Sites was necessary, having regard to the criteria established and applied by the Court under Article 10 of the Convention. Such an obligation, however, flows directly from the Convention and from the case-law of the Convention institutions. In reaching their decision, the courts simply found it established that the only means of blocking access to the offending website in accordance with the order made to that effect was to block all access to Google Sites (see paragraphs 8, 10 and 13 above). However, in the Court's view, they should have taken into consideration, among other elements, the fact that such a measure, by rendering large quantities of information inaccessible, substantially restricted the rights of Internet users and had a significant collateral effect.

67. In the light of these considerations and of its examination of the legislation in question as applied in the instant case, the Court concludes that the interference resulting from the application of section 8 of Law no. 5651 did not satisfy the foreseeability requirement under the Convention and did not afford the applicant the degree of protection to which he was entitled by the rule of law in a democratic society. Furthermore, the provision in question appears to be in direct conflict with the actual wording of paragraph 1 of Article 10 of the Convention, according to which the rights set forth in that Article are secured "regardless of frontiers" (see, to the same effect, *Association Ekin*, cited above, § 62).

68. The Court further observes that the measure in question produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all the sites hosted by Google Sites. Furthermore, the judicial review procedures concerning the blocking of Internet sites are insufficient to meet the criteria for avoiding abuse, as domestic law does not provide for any

safeguards to ensure that a blocking order in respect of a specific site is not used as a means of blocking access in general.

69. Accordingly, there has been a violation of Article 10 of the Convention.

70. In view of that conclusion, the Court does not consider it necessary in the instant case to examine whether the other requirements of paragraph 2 of Article 10 have been met.

II. ALLEGED VIOLATION OF ARTICLES 6, 7 AND 13 OF THE CONVENTION AND ARTICLE 2 OF PROTOCOL No. 1

71. Relying on Articles 6 and 13 of the Convention, the applicant complained that he had not had an effective judicial remedy enabling him to have the impugned measure reviewed by the courts and have possible abuse by the authorities censured.

The applicant also alleged an infringement of the principle that only the law can define a crime and prescribe a penalty, enshrined in Article 7 of the Convention.

Lastly, from the standpoint of Article 2 of Protocol No. 1, he complained of an infringement of his right to education, arguing that the prohibition in question had prevented him from pursuing his studies for his doctorate.

72. In view of its finding of a violation under Article 10 of the Convention (see paragraph 69 above), the Court considers that it has examined the main legal questions raised in the present case. In the light of all the facts of the case, it deems it unnecessary to rule separately on either the admissibility or the merits of the complaints under Articles 6, 7 and 13 of the Convention and Article 2 of Protocol No. 1 (see *Recep Kurt v. Turkey*, no. 23164/09, § 70, 22 November 2011, and *Kamil Uzun v. Turkey*, no. 37410/97, § 64, 10 May 2007).

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

73. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

74. The applicant claimed 10,000 euros (EUR) in respect of non-pecuniary damage.

75. The Government contested the applicant's claim.

76. The Court considers it appropriate to award the applicant EUR 7,500 in respect of non-pecuniary damage.

B. Costs and expenses

77. The applicant also claimed EUR 3,300 for the costs and expenses incurred before the domestic courts and before the Court. He asserted in particular that the presentation of his case before the domestic courts and the Strasbourg institutions had entailed over 28 hours' work at an hourly rate of 250 Turkish liras, in accordance with the scale of minimum fees of the Istanbul and İzmir Bars.

78. The Government contested those claims.

79. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and its case-law, the Court considers it reasonable to award the applicant the sum of EUR 1,000 covering costs under all heads.

C. Default interest

80. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Declares* admissible the complaint concerning the interference with the applicant's freedom to receive and impart information;

2. *Holds* that there has been a violation of Article 10 of the Convention;

3. *Holds* that there is no need to examine separately the admissibility or merits of the complaints under Articles 6, 7 and 13 of the Convention and Article 2 of Protocol No. 1;

4. *Holds*

   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, the following amounts, to be converted into Turkish liras at the rate applicable at the date of settlement:

(i) EUR 7,500 (seven thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
(iii) EUR 1,000 (one thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in French, and notified in writing on 18 December 2012, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Stanley Naismith
Registrar

Guido Raimondi
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Pinto de Albuquerque is annexed to this judgment.

G.RA.
S.H.N.

CONCURRING OPINION OF JUDGE PINTO DE ALBUQUERQUE

The *Ahmet Yıldırım* case is about collateral Internet blocking. It involves an *interim* court injunction blocking access for all Turkish-based users to the Google Sites domain[1], including the applicant's personal website which was hosted by that domain. In fact, this is the first time the question of freedom of expression on Web 2.0-based platforms has been put to the European Court of Human Rights ("the Court"). I agree with the finding of a violation of Article 10 of the European Convention on Human Rights ("the Convention"), but I am convinced that the reasoning of the judgment does not set forth, as it should, the fundamental principles applicable to restrictions on freedom of expression in this field[2]. The purpose of this opinion is to supplement the judgment by setting out those principles, the importance of which is emphasised by two obvious reasons: firstly, the scant case-law of the Court on this topic demands a principled approach to these novel and complex issues in order to avoid erratic, or even contradictory, case-law; secondly, in view of the deficient legislative framework of the respondent State, which will require legislative reform, there is a pressing need for clear guidelines in accordance with the Court's standards applicable in this field.

The interference with the applicant's freedom of expression

The decision of the Denizli Criminal Court of First Instance of 23 and 24 June 2009 constituted interference with the applicant's freedom of expression inasmuch as it blocked access to Google Sites, the domain he had used to create his own site. The measure was based on section 8(1)(b) of Law no. 5651. It was taken within the framework of a set of criminal proceedings opened to investigate another site created in Google Sites, which included content considered offensive to the memory of Mustafa Kemal Atatürk. The Court has no information concerning any notification or attempted notification of Google Inc., the US-based owner and operator of Google Sites, prior to the issuing of the blocking order.

Regardless of the allegedly illegal content of the site on Atatürk[3], the fact is that the applicant's site included only his academic works and other texts

1. Google Sites is a component of a software package known as Google Apps, which furnishes the tools for creating and maintaining personal websites.
2. Although Internet blocking orders may jeopardise various human rights, such as the access provider's right to property, the content provider's freedom of expression and the user's freedom of information, in this particular case the focus will be on the second aspect.
3. The political and historical nature of the publications on Atatürk should also have been taken into account (for the differences between a speech on "established historical facts"

and personal opinions on various topics such as the social Web, the semantic Web, complex networks, complex systems and the philosophy of science. The blocking order failed to take into consideration that fact and consequently the fact that the applicant's site, as many others based on Google Sites, had no connection whatsoever with the site which had been at the origin of the criminal proceedings.

The European standards for the blocking of Internet publications

The Council of Europe standards on freedom of expression on the Internet have been established in various Resolutions, Recommendations and Declarations, in addition to the Convention on Cybercrime and its Additional Protocol[1]. Of these documents, the following three are of the utmost importance for the issues at stake in the present case.

---

and an ongoing debate on historical facts, see my separate opinion in *Fáber v. Hungary*, no. 40721/08, 24 July 2012).

1. The relevant hard and soft law includes the Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), the Declaration by the Committee of Ministers on the protection of freedom of expression and information and freedom of assembly and association with regard to Internet domain names and name strings, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member States on the protection and promotion of the universality, integrity and openness of the Internet, the Declaration by the Committee of Ministers on Internet governance principles, the Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and online service providers, Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services, the Declaration of the Committee of Ministers on the Digital Agenda for Europe, the Declaration of the Committee of Ministers on network neutrality, the Declaration of the Committee of Ministers on the management of Internet Protocol address resources in the public interest, the Declaration of the Committee of Ministers on enhanced participation of member States in Internet governance matters, the Human Rights Guidelines for online games providers, the Human Rights Guidelines for Internet service providers, Recommendation CM/Rec(2008)6 of the Committee of Ministers on measures to promote the respect for freedom of expression and information with regard to Internet filters, Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet, the Declaration on freedom of communication on the Internet adopted by the Committee of Ministers on 28 May 2003, Recommendation 1586 (2002) of the Parliamentary Assembly on the digital divide and education, Recommendation No. R (2001) 8 of the Committee of Ministers on self-regulation concerning cyber content, Recommendation 1543 (2001) of the Parliamentary Assembly on racism and xenophobia in cyberspace, the Declaration on a European policy for new information technologies adopted by the Committee of Ministers on 7 May 1999, Recommendation No. R (99) 14 of the Committee of Ministers on universal community service concerning new communication and information services, Recommendation No. R (99) 5 for the protection of privacy on the Internet, Recommendation 1332 (1997) of

– Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines, which provides that:

> "12. A prerequisite for the existence of effective search engines is the freedom to crawl and index the information available on the Web. The filtering and blocking of Internet content by search-engine providers entails the risk of violation of freedom of expression guaranteed by Article 10 of the Convention in respect to the rights of providers and users to distribute and access information.
>
> 13. Search-engine providers should not be obliged to monitor their networks and services proactively in order to detect possibly illegal content, nor should they conduct any *ex ante* filtering or blocking activity, unless mandated by court order or by a competent authority. However, there may be legitimate requests to remove specific sources from their index, for example in cases where other rights outweigh the right to freedom of expression and information; the right to information cannot be understood as extending the access to content beyond the intention of the person who exercises her or his freedom of expression.
>
> ...
>
> 16. In addition, member States should work with search-engine providers so that they:
>
> – ensure that any necessary filtering or blocking is transparent to the user. The blocking of all search results for certain keywords should not be included or promoted in self- and co-regulatory frameworks for search engines. Self- and co-regulatory regimes should not hinder individuals' freedom of expression and right to seek, receive and impart information, ideas and content through any media. As regards the content that has been defined in a democratic process as harmful for certain categories of users, member States should avoid general de-indexation which renders such content inaccessible to other categories of users. In many cases, encouraging search engines to offer adequate voluntary individual filter mechanisms may suffice to protect those groups;
>
> – explore the possibility of allowing de-indexation of content which, while in the public domain, was not intended for mass communication (or mass communication in aggregate)."

– Recommendation CM/Rec(2008)6 of the Committee of Ministers to member States on measures to promote the respect for freedom of expression and information with regard to Internet filters, according to which:

---

the Parliamentary Assembly on the scientific and technical aspects of the new information and communications technologies, Recommendation No. R (97) 19 of the Committee of Ministers on the portrayal of violence in the electronic media, Recommendation 1314 (1997) of the Parliamentary Assembly on the new technologies and employment, Resolution 1120 (1997) of the Parliamentary Assembly on the impact of the new communication and information technologies on democracy, Recommendation No. R (95) 13 of the Committee of Ministers concerning problems of criminal procedural law connected with information technology, Recommendation No. R (92) 15 of the Committee of Ministers concerning teaching, research and training in the field of law and information technology, and Recommendation 1122 (1990) of the Parliamentary Assembly on the revival of the countryside by means of information technology.

"III. Use and application of Internet filters by the public and private sector

Notwithstanding the importance of empowering users to use and control filters as mentioned above, and noting the wider public-service value of the Internet, public actors on all levels (such as administrations, libraries and educational institutions) which introduce filters or use them when delivering services to the public, should ensure full respect for all users' right to freedom of expression and information and their right to private life and secrecy of correspondence.

In this context, member States should:

i. refrain from filtering Internet content in electronic communications networks operated by public actors for reasons other than those laid down in Article 10, paragraph 2, of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;

ii. guarantee that nationwide general blocking or filtering measures are only introduced by the State if the conditions of Article 10, paragraph 2, of the European Convention on Human Rights are fulfilled. Such action by the State should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body, in accordance with the requirements of Article 6 of the European Convention on Human Rights;

iii. introduce, where appropriate and necessary, provisions under national law for the prevention of intentional abuse of filters to restrict citizens' access to lawful content;

iv. ensure that all filters are assessed both before and during their implementation to ensure that the effects of the filtering are proportionate to the purpose of the restriction and thus necessary in a democratic society, in order to avoid unreasonable blocking of content;

v. provide for effective and readily accessible means of recourse and remedy, including suspension of filters, in cases where users and/or authors of content claim that content has been blocked unreasonably;

vi. avoid the universal and general blocking of offensive or harmful content for users who are not part of the group which a filter has been activated to protect, and of illegal content for users who justifiably demonstrate a legitimate interest or need to access such content under exceptional circumstances, particularly for research purposes;

vii. ensure that the right to private life and secrecy of correspondence is respected when using and applying filters and that personal data logged, recorded and processed via filters are only used for legitimate and non-commercial purposes."

– Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, which provides as follows:

"III. Openness

Member States should affirm freedom of expression and the free circulation of information on the Internet, balancing them, where necessary, with other legitimate rights and interests, in accordance with Article 10, paragraph 2, of the European Convention on Human Rights as interpreted by the European Court of Human Rights, by:

– promoting the active participation of the public in using, and contributing content to, the Internet and other ICTs;

– promoting freedom of communication and creation on the Internet, regardless of frontiers, in particular by:

a. not subjecting individuals to any licensing or other requirements having a similar effect, nor any general blocking or filtering measures by public authorities, or restrictions that go further than those applied to other means of content delivery;

b. facilitating, where appropriate, 're-users', meaning those wishing to exploit existing digital content resources in order to create future content or services in a way that is compatible with respect for intellectual property rights;

c. promoting an open offer of services and accessible, usable and exploitable content via the Internet which caters to the different needs of users and social groups, in particular by:

– allowing service providers to operate in a regulatory framework which guarantees them non-discriminatory access to national and international telecommunication networks;

– increasing the provision and transparency of their online services to citizens and businesses;

– engaging with the public, where appropriate, through user-generated communities rather than official websites;

– encouraging, where appropriate, the re-use of public data by non-commercial users, so as to allow every individual access to public information, facilitating their participation in public life and democratic processes;

– promoting public-domain information accessibility via the Internet which includes government documents, allowing all persons to participate in the process of government; information about personal data retained by public entities; scientific and historical data; information on the state of technology, allowing the public to consider how the information society might guard against information warfare and other threats to human rights; creative works that are part of a shared cultural base, allowing persons to participate actively in their community and cultural history;

– adapting and extending the remit of public-service media, in line with Recommendation Rec(2007)3 of the Committee of Ministers to member States on the remit of public-service media in the information society, so as to cover the Internet and other new communication services and so that both generalist and specialised contents and services can be offered, as well as distinct personalised interactive and on-demand services."

In the Court's case-law, three cases to date have dealt specifically with Internet publications[1].

In *K.U. v. Finland*, the Court held as follows:

1. In *Mouvement raëlien suisse v. Switzerland* ([GC], no. 16354/06, ECHR 2012), faced with a case in which the national authorities, after examining the applicant association's website, mentioned on a poster, and other sites that were accessible via hyperlinks on the applicant's site, proceeded to prohibit a particular form of expression of the applicant association, the majority did not address this issue, which was analysed in various separate opinions.

> "Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context."[1]

In *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, the Court stated:

> "In the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10."[2]

Lastly, in *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, the Court found:

> "... the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a 'public watchdog' ... "[3]

In the light of these documents and the practice of the States Parties referred to in the judgment's reasoning, the minimum criteria for Convention-compatible legislation on Internet blocking measures are: (1) a definition of the categories of persons and institutions liable to have their publications blocked, such as national or foreign owners of illegal content, websites or platforms, users of these sites or platforms and persons providing hyperlinks to illegal sites or platforms which have endorsed them[4]; (2) a definition of the categories of blocking orders, such as blocking of entire websites, Internet Protocol (IP) addresses, ports, network protocols or types of use, like social networking[5]; (3) a provision on the territorial

1. *K.U. v. Finland*, no. 2872/02, § 49, ECHR 2008.
2. *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, nos. 3002/03 and 23676/03, § 27, ECHR 2009.
3. *Editorial Board of* Pravoye Delo *and Shtekel v. Ukraine*, no. 33014/05, § 64, ECHR 2011.
4. The distinction between a content and a service provider is not always straightforward. For instance, when the service provider interferes with the content provided by a third person, the service provider in turn becomes a content provider. The legislature should provide a clear legal definition of both, since their responsibilities are also different.
5. The possibilities range from more sophisticated blocking orders aimed at IP addresses, port numbers, URLs or content data to less sophisticated ones like blocking certain domain names on the corresponding servers or specific entries on the hit list of search engines.

ambit of the blocking order, which may have region-wide, nationwide, or even worldwide effect[1]; (4) a limit on the duration of the blocking order[2]; (5) an indication of the "interests", in the sense of one or more of those included in Article 10 § 2 of the Convention, that may justify the blocking order; (6) observance of the criterion of proportionality, which provides for a fair balancing of freedom of expression and the competing "interests" pursued, while ensuring that the essence (or minimum core) of freedom of expression is respected[3]; (7) compliance with the principle of necessity, which enables an assessment to be made as to whether the interference with freedom of expression adequately advances the "interests" pursued and goes no further than is necessary to meet the said "social need"[4]; (8) definition of the authorities competent to issue a reasoned blocking order[5]; (9) a procedure to be followed for the issuance of that order, which includes the examination by the competent authority of the case file supporting the request for a blocking order and the hearing of evidence from the affected person or institution, unless this is impossible or incompatible with the "interests" pursued[6]; (10) notification of the blocking order and the grounds for it to the person or institution affected; and (11) a judicial appeal procedure against the blocking order[7].

This framework must be established via specific legal provisions; neither the general provisions and clauses governing civil and criminal

1. On the right to cross-border access to information, see *Khurshid Mustafa and Tarzibachi v. Sweden*, no. 23883/06, §§ 44-50, 16 December 2008, and the Committee of Ministers Declaration on freedom of communication on the Internet, 28 May 2003, Principle 3.

2. Indefinite or indeterminate Internet blocking orders constitute *per se* unnecessary interference with freedom of expression.

3. For instance, the blocking of a Holocaust-denying site is proportionate (see the French Court of Cassation decision no. 707 of 19 June 2008, 07-12244).

4. That less draconian measures should be envisaged, such as the confiscation of particular issues of the newspapers or restrictions on the publication of specific articles, has already been determined in *Ürper and Others v. Turkey* (nos. 14526/07, 14747/07, 15022/07, 15737/07, 36137/07, 47245/07, 50371/07, 50372/07 and 54637/07, § 43, 20 October 2009). The same principle is applicable to the blocking of publications, for example by implementing a "notice and take down" policy prior to the issuance of a blocking order. In the field of the Internet, an additional factor to be considered is the fact that some blocking measures may easily be circumvented, which makes the necessity of the measure questionable.

5. The fact that multiple institutions, bodies and persons may issue blocking orders proves detrimental to legal certainty. The concentration of blocking powers in one single authority facilitates uniform application of the law and closer monitoring of the practice.

6. For the relevance of the guarantee that evidence be heard from the affected persons, see decision no. 2009-580 DC of the French Constitutional Council of 10 June 2009, paragraph 38.

7. For the importance of similar guarantees of notification and appeal, see decision no. 2011-625 DC of the French Constitutional Council of 10 March 2011, paragraph 8.

responsibility nor the e-commerce Directive[1] constitute a valid basis for ordering Internet blocking. In any case, blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security[2]. Thus, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails *per se* the "adequacy" test, in so far as it lacks a "rational connection", that is, a plausible instrumental relationship between the interference and the social need pursued[3]. By the same token, blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship[4].

When exceptional circumstances justify the blocking of illegal content, it is necessary to tailor the measure to the content which is illegal and avoid targeting persons or institutions that are not *de jure* or *de facto* responsible for the illegal publication and have not endorsed its content. In the case of

1. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the Directive on electronic commerce) does not deal with the issuance of blocking orders and its conditions, and the only reference it makes in this regard is to state that "in Member States which authorise unsolicited commercial communications by electronic mail, the setting up of appropriate industry filtering initiatives should be encouraged and facilitated" and that "[t]his Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information" (Recital 30 of the Preamble and Articles 12 § 3, 13 § 2 and 14 § 3).

2. See United Nations Human Rights Committee General Comment No. 34, UN Doc. CCPR/C/GC/34, paragraph 43; the Joint Declaration on Freedom of Expression and the Internet by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information; and the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 10 August 2011, UN Doc. A/66/290, paragraphs 37-44.

3. Committee of Ministers Declaration on freedom of communication on the Internet, 28 May 2003, Principle 3, and United Nations Human Rights Committee General Comment No. 34, cited above, paragraph 22.

4. The inadmissibility of prohibitions on the future publication of entire newspapers whose content was unknown at the time of the national courts' decisions has been established in *Ürper and Others*, cited above, § 42. The blocking of a website or a platform and the future publication of articles thereon whose content was unknown at the time of the decision is equivalent to the above-mentioned prohibition regarding a newspaper. Thus, the rationale of *Ürper and Others* applies to the blocking of websites or platforms and *a fortiori* to the collateral suppression of legal websites and platforms.

interim or preventive measures which are based on reasonable grounds to suspect the commission of a crime, freedom of expression warrants not only a particularly tight legal framework ("*cadre légal particulièrement strict*") but also the most careful scrutiny by the courts, and consequently the exercise of special restraint[1]. None of these guarantees was provided by the impugned decisions of the national courts, as will be shown.

The application of the European standards to the instant case

Law no. 5651 lays down only the following criteria for the issuance of an Internet blocking order: the nature of the criminal offences or activities which may give rise to a blocking order, the degree of evidence necessary for a blocking order to be issued ("sufficient grounds to suspect"), the competence of the judge, the court or, in urgent matters, the public prosecutor to issue the blocking order, an appeal against that order[2] and its termination when the accused is acquitted, the case is dismissed or the illegal content is deleted. Thus, the national legislation, although not arbitrary, since it entrusts to the judiciary the power to block or not to block, is at least very deficient, because it does not surround the exercise of judicial power with all the required conditions and safeguards and therefore does not afford basic guarantees of freedom of expression to Internet content providers.

It is a fact that the domestic courts were, and still are, obliged to respect freedom of expression, as interpreted by the Court's case-law, and thus should have interpreted restrictively their own powers under section 8 of Law no. 5651. But they failed to do so. It is particularly regrettable that they omitted to advance any argument justifying the notion that the public interest in blocking access outweighed the applicant's freedom of expression or any consideration of the existence of a clear and imminent danger resulting from the applicant's publication. It is also to be regretted

1. On the legal framework, see *RTBF v. Belgium*, no. 50084/06, § 115, ECHR 2011: "if prior restraints are required in the media sphere, they must form part of a legal framework ensuring both tight control over the scope of any bans and effective judicial review to prevent potential abuses." And on the judicial exercise of restraint, see Observer *and* Guardian *v. the United Kingdom*, 26 November 1991, § 60, Series A no. 216: "... the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court. This is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest." This was confirmed by *Editions Plon v. France*, no. 58148/00, § 42, ECHR 2004-IV; *Association Ekin v. France*, no. 39288/98, § 56, ECHR 2001-VIII; and *Obukhova v. Russia*, no. 34736/03, § 22, 8 January 2009. And in the American case-law, see *New York Times Co. v. United States*, 403 US 713 (1971), and particularly the concurring opinion of Justice Brennan (the US Constitution "tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result").

2. But no provision is made for giving notice of the blocking order to the affected parties.

that the Denizli Criminal Court of First Instance decision of 13 July 2009 rejected the applicant's application to set aside the order with the argument that no other less intrusive measure was available.

If the interference with the applicant's freedom of expression on the public forum of the Internet must be assessed in terms of the negative obligations arising from Article 10 of the Convention, which already narrows the breadth of the margin of appreciation of the respondent State[1], the interim and preventive nature of the contested blocking measure narrows it even further. The fact that this measure is, according to the law, based on the existence of "sufficient grounds to suspect" that the publications on the Internet constitute certain crimes points not only to the precarious nature of the assessment (a mere "suspicion") which the courts are called upon to perform, but also to the limited amount of evidence ("sufficient" grounds) required to support the issuance of the measure. The particular judicial restraint warranted by the provisional nature of the measure and by the very deficient legal framework was entirely absent[2].

Conclusion

To borrow the words of *Banatan Books, Inc.*, any prior restraint on expression on the Internet comes to me with a heavy presumption against its Convention validity[3]. In the instant case, the respondent Government did not satisfy the burden of showing that the imposition of such a restraint was justified.

Having regard to the State's negative obligation to refrain from interfering with the applicant's freedom of expression on the Internet, to the application of Law no. 5651 by the domestic courts without any consideration of the Convention principles, to the lawful form and nature of the material published by the applicant and to the lack of any connection between his site and the allegedly illegal site, and after assessing the reasons given by the national authorities in the light of their narrow margin of appreciation, I find that there has been a violation of the applicant's freedom of expression enshrined in Article 10 of the Convention.

In view of the insufficient guarantees provided by Law no. 5651 with regard to the blocking of Internet publications, I would also have found it established, based on Article 46, that the respondent State has a duty to amend the legislation in line with the standards set out above.

1. See my separate opinion in *Mouvement raëlien suisse*, cited above.
2. According to the Report of the OSCE Representative on Freedom of the Media on Turkey and Internet censorship, this unrestrained attitude has been common practice.
3. *Banatan Books, Inc. v. Sullivan*, 372 US 58 (1963).