Council of the
European Union

Brussels, 9 November 2015
(OR. en)

13744/15

JAI 821
FREMP 243

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
Subject:	Ensuring the respect for the rule of law - Dialogue and exchange of views

For the purposes of COREPER on 11 November 2015 and the Council (General Affairs) on 17 November 2015, delegations will find in Annex I the discussion paper of the Presidency on "Ensuring the respect for the rule of law" and in Annex II the discussion paper of the Presidency on "The rule of law in the age of digitalisation."

ANNEX

General Affairs Council

17 November 2015

Discussion Paper

Ensuring the respect for the Rule of Law

ENSURING RESPECT FOR THE RULE OF LAW

The European Union is based on the rule of law: every action taken by it is founded on the Treaties approved voluntarily and democratically by all EU Member States. In December 2014, the Council and the Member States meeting within the Council adopted conclusions on ensuring respect for the rule of law within the European Union.

They committed themselves to establishing a dialogue among all Member States within the Council to promote and safeguard the rule of law in the framework of the Treaties and underlined that this dialogue would be based on the principles of objectivity, non-discrimination and equal treatment of all Member States.

They also agreed that this dialogue would be based on a non-partisan and evidence-based approach and emphasised that such an approach will be without prejudice to the principle of conferred competences, as well as the respect of national identities of Member States inherent in their fundamental political and constitutional structures, inclusive of regional and local self-government, and their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security, and should be brought forward in light of the principle of sincere cooperation.

Furthermore, they agreed that this dialogue will be developed in a way which is complementary to work undertaken in other EU Institutions and international organizations, avoiding duplication and taking into account existing instruments and expertise in this area.

The Luxembourg Presidency, while ensuring the full respect of the principles mentioned above, intends to organize this first political dialogue in an inclusive approach.

- In the introductory part of this first dialogue, the Commission will present the outcome of its **annual colloquium on fundamental rights "Tolerance and respect: preventing and combating anti-Semitic and anti-Muslim hatred in Europe" that took place on 1-2 October 2015.**

- After that presentation, all Member States are invited to share **one example of a best practice and one example of a challenge encountered at national level in relation to the respect for the rule of law, as well as the approach to respond to that challenge.**

- Finally, delegations will have the opportunity to react to the Presidency non-paper **"The rule of law in the age of digitalization" by indicating in which area they see a need for EU action to further strengthen the rule the law.**

ANNEX II

General Affairs Council

17 November 2015

Discussion Paper

The Rule of Law

in the Age of Digitalization

THE RULE OF LAW IN THE AGE OF DIGITALIZATION

Growing numbers of citizens in the European Union rely on information and communication technologies (ICTs) and the Internet as essential tools for their everyday activities. Citizens therefore expect the Internet and the ICT infrastructure and services to be open, accessible, affordable, secure and reliable. In addition, they expect that the fundamental values of the European Union and the rule of law are fully preserved and protected.

For the Luxembourg Presidency, **the dialogue on the rule of law between all the Member States** and **the development of the Digital Single Market (DSM)** are among the key priorities for the second semester 2015.[1] The discussion paper "The rule of law in the age of digitalization" combines the two themes in an attempt to identify areas in the digital environment where the rule of law could be strengthened in a useful and sustainable way.

THE RULE OF LAW IN THE UNION

The term "rule of law" refers to a principle of governance by which all persons, institutions and entities, public and private, including the state itself, are accountable to laws that are publicly promulgated, equally enforced, independently adjudicated and consistent with international human rights norms and standards. Moreover, the rule of law entails adherence to a number of principles: be it supremacy of law, equality before the law, accountability to the law, fairness in applying the law, separation of powers, participation in decision making, legal certainty, avoidance of arbitrariness or procedural and legal transparency.[2]

---

1 Luxembourg Presidency, A Union for the citizens – Priorities of the Luxembourg Presidency, p. 16, 19.

2 UN Secretary-General, Report « The rule of law and transitional justice in conflict and post-conflict societies », 23 August 2004, p. 4. Available at: http://www.unrol.org/files/2004%20report.pdf.

In the preamble to the Treaty on European Union (TEU), the signatory states emphasized the need to draw inspiration from the cultural, religious and humanist inheritance of Europe. It is from this inheritance that the universal values of the inviolable and inalienable rights of the human person, freedom, democracy, equality and **the rule of law** have been developed.

Article 2 TEU specifies the values on which the EU is founded: respect for human dignity, freedom, democracy, equality, **the rule of law** and respect for human rights, including the rights of persons belonging to minorities. The Treaty furthermore states that "these values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."[3]

The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adopted on 12 December 2007. Accordingly, it has the same legal value as the Treaties.[4] The Charter represents a catalogue of civil, political, economic and social rights, which are legally binding not only on the Union and its institutions, but also on the Member States when it comes to the implementation of EU law. The preamble of the Charter states that the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity. Most importantly, it places the individual at the heart of its activities, by establishing the citizenship of the Union and by creating an area of freedom, security and justice.[5]

---

3 Article 2 TEU.
4 Article 6 (1) TEU.
5 Charter of Fundamental Rights of the European Union, preamble.

THE DIGITAL SINGLE MARKET STRATEGY OF THE UNION

The European Council has on several occasions underlined the strategic character of the **DSM** and the necessity to fully exploit the potential of the digital economy and digital technologies by 2015. The new President of the European Commission identified the completion of the **DSM** as one of its ten political priorities.[6] The overall objective is to work towards a market in which the individuals and companies can seamlessly access and exercise online cross-border activities under conditions of fair competition and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. The Digital Single Market strategy,[7] adopted on 6 May 2015, includes 16 initiatives to be delivered by the end of 2016. The DSM will built on three pillars: firstly a better access for consumers and business to online goods and services, secondly, creating the conditions for digital networks and services to flourish and last but not least, maximizing the growth potential. Ensuring the rule of law in the digital environment has an important role to play in achieving these objectives in the context of the DSM.

---

6 Jean-Claude Juncker, A new start for Europe: My agenda for jobs, growth, fairness and democratic change, 15 July 2014. Available at: http://ec.europa.eu/priorities/docs/pg_en.pdf

7 European Commission, A Digital Single Market Strategy for Europe, 6 May 2015. Available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

THE RULE OF LAW IN THE AGE OF DIGITALIZATON

The rule of law is essential in the building of an inclusive and open digital society in the European Union and beyond. The basic requirements of the rule of law must apply equally both online and offline. For the purpose of defining a framework for this discussion paper, building on the ongoing work of the Council of Europe,[8] the Presidency proposes to examine in greater detail the following themes:

- Freedom of expression
- Internet governance
- Data protection
- Cybersecurity

These themes, central to the strengthening of the rule of law in the age of digitalization, are highly complex and closely intertwined.

[8] Council of Europe, Commissioner for Human Rights, "The rule of law on the Internet and in the wider digital world," December 2014. Available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2734552&SecMode=1&DocId=2262340&Usage=2

FREEDOM OF EXPRESSION

According to the Universal Declaration of Human Rights, freedom of expression is the right of every individual to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.[9]

The European Convention for the Protection of Human Rights and Fundamental Freedoms[10] also states that everyone has the right to freedom of expression. It also states that this right includes the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The Convention furthermore stipulates in Article 10 that the exercise of these freedoms, given that it carries with it duties and responsibilities, may be subject to formalities, conditions, restrictions or penalties that are prescribed by law. These are also necessary in a democratic society, be it 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.

Similarly, the Charter of Fundamental Rights of the European Union refers to the freedom of expression and information and declares that everyone has the right to freedom of expression. Furthermore, it states that "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."[11]

In practice, however, it can happen that under certain circumstances the freedom of expression is restricted through measures that include censorship, restrictive press legislation, and harassment of journalists, whistleblowers, bloggers and others who voice their opinions, as well as crackdowns on religious minorities and other forms of suppression of religious freedom. The freedom of expression and its articulation with national legislation about online activities, such as the liability of Internet intermediaries, is a constant challenge.

---

9 United Nations, the Universal Declaration of Human Rights, 10 December 1948. Available at: http://www.un.org/Overview/rights.html

10 Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms. Available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf

11 Charter of Fundamental Rights of the European Union, Article 11 (1).

Online the freedom of expression is often challenged in situations where content may need to be removed, be it for considerations of privacy, intellectual property rights or for other reasons. This puts Internet intermediaries and their liability in conflictual situations of having to find a balance between different fundamental rights.

Possible restrictions to the freedom of expression are also rooted in two other instruments of international law: the International Convention on the Elimination of All Forms of Racial Discrimination (CERD)[12] and the International Covenant on Civil and Political Rights (ICCPR).[13] Article 4 (a) of the CERD obligates signatories to make "all dissemination of ideas based on racial superiority or hatred" a punishable offense, while Article 20 of the ICCPR requires outlawing “any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence”.

Member States have established legislation designed to curb incitement to racial and religious hatred through hate speech that, in the age of digitalization, is more and more frequently disseminated through ICTs and over the Internet. Apart from the offences covered by the scope of the Framework Decision on racism and xenophobia, [14] there are differences concerning the question what constitutes hate speech.

---

12 International Convention on the Elimination of All Forms of Racial Discrimination, 21 December 1965. Available at: http://www.ohchr.org/Documents/ProfessionalInterest/cerd.pdf

13 International Covenant on Civil and Political Rights, 16 December 1966. Available at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

14 Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328 of 6.12.2008.

Regarding key actions on preventing and combating anti-Semitic and anti-Muslim hatred following the first annual colloquium on fundamental rights, it is proposed to fight hate speech by working with IT companies, civil society and the media and to ensure implementation of hate crime laws and new EU rules on protecting the rights of victims of crime and improving recording and data collection of hate crime incidents.[15] The first coordination meeting with internet platforms and social networks, to be prepared by the Commission's expert group on the implementation of the Framework Decision on racism and xenophobia, will take place on 23 November 2015 in Brussels.

INTERNET GOVERNANCE

The UN-initiated World Summit on the Information Society (WSIS) proposed the following definition of Internet governance as part of the June 2005 report of the working group on Internet governance (WGIG): "Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[16]

The current multi-stakeholder approach to Internet governance takes into account the interests of governments, the private sector, the technical community, academia and civil society. This model promotes inclusiveness and accountability. Internet governance principles stress the need to apply public international law and international human rights law equally both online and offline. They also emphasize the need to respect the rule of law and democracy on the Internet. These principles recognize and promote the multiple stakeholders in Internet governance and, most importantly, urge all public and private actors to uphold human rights in all their operations and activities, including the design of new technologies, services and applications. Finally, they call on states to respect the national sovereignty of other states, and to refrain from actions that would harm persons or entities located outside their territorial jurisdiction.

---

15 European Commission, joining forces against anti-Semitic and anti-Muslim hatred in the EU: outcomes of the first annual colloquium on fundamental rights, 9 October 2015. Available at: http://ec.europa.eu/justice/events/colloquium-fundamental-rights-2015/files/fundamental_rights_colloquium_conclusions_en.pdf

16 Working Group on Internet Governance (WGIG), Report of the Working Group on Internet Governance, Château de Bossey, June 2005. Available at: http://www.wgig.org/docs/WGIGREPORT.pdf

Of course, some of these principles still remain largely declaratory: there is in fact still a deficiency in actual Internet governance arrangements that are aimed at guaranteeing the application of these principles in practice. States should ensure that any restrictions on access to Internet content affecting users under their jurisdiction are based on a strict and predictable legal framework. This framework should have the capability to regulate the scope of any such restrictions and afford the guarantee of judicial oversight to prevent any abuses. Removing content, if necessary, must be effective and proportionate, in particular whether it is targeted enough so as to impact only on the specific content that requires removal. In addition, domestic courts must examine whether any blocking measure is necessary, effective and proportionate, and in particular whether it is targeted enough so as to impact only on the specific content that requires blocking.

DATA PROTECTION

The Treaty on the Functioning of the European Union (TFUE) recalls that everyone has the right to the protection of personal data concerning them and that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[17]

The Luxembourg Presidency aims to finalize the EU data protection reform by the end of the year. The completion and the success of the DSM will largely depend on the trust that citizens and companies have in cross-border flow of data. The EU can be seen as a model for a high level of data protection. This heritage must be strengthened by the adoption of the new regulatory framework. Citizens' rights need to be protected while taking into account the competitiveness of the European economy need to be protected.[18]

---

17 Article 16 TFUE.

18 Luxembourg Presidency, A Union for the citizens – Priorities of the Luxembourg Presidency, p. 16-17.

In its judgment of 8 April 2014, which declared the Directive 2006/24/EC[19] on the retention of data invalid,[20] the Court of Justice of the European Union (CJEU) underlined the importance of fundamental rights (i.e. the right to a private life and the right to the protection of personal data enshrined in the Charter). An adequate response is necessary, taking into account the principles deriving from the case law, which is to be included in the updated legal framework governing data protection. In its judgment of 6 October 2015, the CJEU declared invalid the Commission's U.S. Safe Harbour decision.[21].These decisions of the CJEU demonstrate the preeminence attached to a high level of data protection in the European Union.

Data protection provides the first and most essential backbone for the rule of law in the age of digitalization. Purpose specification and limitation, as well as fairness are core principles of data protection. Compliance with data protection principles and rules must be closely monitored and supervised by independent authorities. States should not impose compulsory retention of data by third parties, including private entities, unless the proportionality principle is fully respected.[22] Retention of communications data must be lawful and balanced parameters for dealing with the scope of data capture, the triggers for access, the retention periods and oversight, for example, are needed, in accordance with the proportionality principle as interpreted by the CJEU in the above-mentioned cases.

---

19 Directive 2006/24/EC. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

20 Court of Justice of the European Union, Press Release No. 54/14, 8 April 2014. Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

21 Court of Justice of the European Union, Press Release No. 117/15, 6 October 2015. Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

22 Charter of Fundamental Rights of the European Union, Article 52.

CYBERSECURITY

Cybersecurity is an essential prerequisite in an environment where digital networks and services can prosper. States have recognized rather late the importance of the Internet with regard to their traditional roles and responsibilities. It is only by working closely with all stakeholders that the online environment can effectively be safeguarded for future generations. Recent cyber hijacking cases[23] and constant cyber-attacks on governments and private companies worldwide show that cyber operations have become a tool for power manipulation and political coercion for states and non-state actors alike.

Cybercrime consists of criminal acts that are committed online by using ICTs or the Internet. It is a borderless problem that can be classified in different categories: crimes specific to the Internet (attacks against information systems or phishing), online fraud and forgery (identity theft, spam and malicious code) and illegal online content (including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia).

[23] TV5 Monde and Sony Pictures can be considered as examples.

The European Union has elaborated an EU Cybersecurity Strategy[24] and the proposed Network and Information Security (NIS) Directive will increase cooperation between Member States as well as improve preparedness of all stakeholders, including governments. Several EU legislative actions contribute to the fight against cybercrime. These include Directives on attacks against information systems[25] and on combating sexual exploitation of children online and child pornography,[26] the ePrivacy Directive[27] and the Framework Decision combating fraud and counterfeiting.[28]

Regarding the Directive on attacks against information systems, a reference to the full respect of the rule of law is made when it comes to fostering and improving cooperation between service providers, producers, law enforcement bodies and judicial authorities.

The European Cybercrime Center (EC3), which started operations in January 2013, acts as the focal point in the fight against cybercrime in the European Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary.

One of the most important challenges is the reconciliation of effective law enforcement powers with the protection of fundamental rights. States must fully comply with international human rights obligations in defining cybercrime in any criminal investigation or prosecutions, also in relation to mutual legal assistance and extradition.[29]

---

24 European Parliament, Council of the European Union, European Economic and Social Committee, European Committee of the Regions, Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace, 2013. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013JC0001&from=EN

25 Directive 2013/40/EU. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

26 Directive 2011/92/EU. Available at : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32011L0093&from=EN

27 Directive 2009/136/EC. Available at : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

28 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32001F0413&from=EN

29 Council of Europe, Commissioner for Human Rights, *op. cit.*, p. 22.

If a state takes action that affects individuals outside its territory, it has to fulfill its obligations in the same way as it would within its national jurisdiction and has to respect international agreements.[30] Apart from content considered illegal under international law, states should only exercise jurisdiction over foreign digital materials in limited circumstances, especially when there is a clear and close nexus between the material and/or the disseminator and the state in question.

CONCLUSION

The digital world is a part of our daily life. Information and communication technologies and the Internet can support the rule of law, but they can also encourage breaching it. The European Union is based on the rule of law: every action taken by it is founded on the Treaties approved voluntarily and democratically by all EU Member States. The Union therefore has an important role to play and a particular responsibility to assume at the global level in defining the general rules and principles in the digital world.

The discussion paper shows that there is ample room for initiatives at EU level to make the DSM fully function as well as to further strengthen the rule of law in the age of digitalization.

---

30 e.g. the European Extradition Convention or the European Convention on Mutual Assistance in Criminal Matters.