

# FOLLOW-UP TO THE COMPARATIVE STUDY ON “BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT”

Dariia Opryshko

Ph.D., media lawyer - Advocate at London Tech Advocates & Global Tech Advocates

## REPORT

*The present research provides an update to this study and reflects the developments in law and practice of Ukraine that have taken place from October 2015 till June 2020.*

## UKRAINE

### 1. Legal Sources

In December 2015 the Council of Europe published a Comparative study on blocking, filtering and take-down of illegal internet content, as carried out by the Swiss Institute of Comparative Law.<sup>1</sup> The present research provides an update to this study and reflects the developments in law and practice of Ukraine that have taken place from October 2015 till June 2020.

As before, issues related to blocking, filtering and take-down of illegal internet content in Ukraine are still regulated by general provisions enshrined in different legislative acts. During the researched period, no special law regulating freedom of expression on the internet has been adopted.

Several legislative acts containing provisions on blocking, filtering and take-down of illegal internet content have been amended in the relevant parts, namely: the Criminal Code,<sup>2</sup> the Criminal Procedural Code,<sup>3</sup> the Civil Procedural Code,<sup>4</sup> the Economic Procedural Code,<sup>5</sup> the Code of Administrative Proceedings,<sup>6</sup> and the Law “On Copyright and Related Rights”.<sup>7</sup>

---

<sup>1</sup> Comparative Study on blocking, filtering and take-down of illegal internet content (2015), available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806554c0>

<sup>2</sup> Criminal Code of Ukraine of 05.04.2001, № 2341-III, Vidomosty Verkhovnoi Rady of Ukraine, 2001, № 25-26, Art.131, available at: <https://zakon.rada.gov.ua/laws/show/2341-14#n1154>

<sup>3</sup> Criminal Procedural Code of Ukraine of 13.04.2012, № 4651-VI, Vidomosty Verkhovnoi Rady of Ukraine, 2013, № 9-10, № 11-12, № 13, Art.88, available at: <https://zakon.rada.gov.ua/laws/show/4651-17>

<sup>4</sup> Civil Procedural Code of Ukraine of 18.03.2004 № 1618-IV, Vidomosty Verkhovnoi Rady of Ukraine, 2004, № 40-41, 42, Art.492, available at: <https://zakon.rada.gov.ua/laws/show/1618-15>

<sup>5</sup> Economic Procedural Code of Ukraine of 06.11.1991 № 1798-XII, Vidomosty Verkhovnoi Rady of Ukraine, 1992, 6, Art.56, available at: <https://zakon.rada.gov.ua/laws/show/1798-12>

<sup>6</sup> Code of Administrative Proceedings of Ukraine of 06.07.2005 № 2747-IV, Vidomosty Verkhovnoi Rady of Ukraine, 2005, № 35-36, №. 37, Art.446, available at: <https://zakon.rada.gov.ua/laws/show/2747-15>

<sup>7</sup> Law of Ukraine “On Copyright and Related Rights” of 23.12.1993 № 3792-XII, Vidomosty Verkhovnoi Rady of Ukraine, 1994, № 13, Art.64, available at: <https://zakon.rada.gov.ua/laws/show/3792-12>

Further changes were introduced at the level of subsidiary regulatory acts – decisions of the National Security and Defence Council of Ukraine and Presidential decrees (see section 2.1.2.).

## **2. Legal Framework**

### **2.1. Blocking and/or Filtering of Illegal Internet Content**

As mentioned above, there is no special law regulating issues related to blocking of internet content in Ukraine. At the same time, Ukrainian legislation allows for blocking of internet content when this is necessary to either protect national security, territorial integrity or public safety, or to stop the dissemination of child sexual abuse content or the violation of copyright and related rights (see sections 2.1.2. and 2.1.3.).

As for filtering of internet content, neither relevant legislation, nor practice exist in Ukraine. Nonetheless, any interested person is free to install software designed for protection from illegal content (e.g. parental control software).

#### **2.1.1. General Legal Framework**

There have not been any substantial changes in the general legal framework since 2015, except for important amendments to the Law “On Copyright and Related Rights” that introduced a “notice and take-down procedure” that applies to the use of some types of content subject to copyright (see section 2.1.3.).

While a number of other amendments to laws and secondary legislation acts aimed at regulating internet-related issues have been proposed, most of them were either dismissed, or shelved.<sup>8</sup>

#### **2.1.2. Protection of National Security, Territorial Integrity or Public Safety**

Without change since 2015, the Law “On Sanctions”<sup>9</sup> stipulates that special economic and other restrictive measures (hereafter – “sanctions”) may be applied to protect national interests, national security, sovereignty and the territorial integrity of Ukraine, to combat terrorism as well as to provide remedy in case of violations of rights, freedoms and lawful interests of Ukrainian citizens, society and the State.

As a new development, based on the Law “On Sanctions” the National Security and Defense Council of Ukraine adopted in 2017 and in 2018 two Decisions on application of individual special economic and other restrictive measures (sanctions) (hereafter – “Decision 2017”<sup>10</sup> and “Decision 2018”<sup>11</sup> respectively). Enacted by Presidential decrees,<sup>12</sup> Decisions 2017 and 2018, among other things, imposed sanctions for the

---

<sup>8</sup> For an overview of legislative initiatives please see: [https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit\\_1.pdf](https://www.ppl.org.ua/wp-content/uploads/2019/04/zvit_1.pdf), <https://bit.ly/2nxBY56>

<sup>9</sup> Law of Ukraine “On Sanctions” of 14.08.2014 No. 1644-VII, Vidomosty Verkhovnoi Rady of Ukraine, 2014, № 40, Art.2018, available at: <https://zakon.rada.gov.ua/laws/show/1644-18#n52>

<sup>10</sup> Decision of the National Security and Defence Council of Ukraine “On application of individual special economic and other restrictive measures (sanctions)” of 28 April 2017, available at: <https://zakon.rada.gov.ua/laws/show/ru/n0004525-17/paran2#n2>

<sup>11</sup> Decision of the National Security and Defence Council of Ukraine “On application and lifting of individual special economic and other restrictive measures (sanctions)” of 2 May 2018, available at: <https://zakon.rada.gov.ua/laws/show/n0006525-18#n2>

<sup>12</sup> Decree of the President of Ukraine “On the Decision of the National Security and Defense Council of Ukraine ‘On application of individual special economic and other restrictive measures (sanctions)’ of 28 April 2017”, of 15 May 2017 No. 133/2017, available at: <https://zakon.rada.gov.ua/laws/show/ru/133/2017/paran2> ; Decree of the

duration of three years on a number of legal entities, mostly of Russian provenance, via which certain web-services and web-resources were carrying out their activities in Ukraine.<sup>13</sup> The sanctions ranged from blocking of assets and restriction of transactions to, notably, blocking access to certain online resources and services operated by the penalised legal entities.

The Law “On Sanctions” does not directly provide for any sanction that would require restricting internet users’ access to services, resources and social-oriented resources, or would oblige internet providers to block access to internet resources, as well as to their subdomains. However, the list of types of sanctions provided for by this Law is non-exhaustive and includes “other sanctions” that must be applied in accordance with the principles set down in this Law (Article 4, part 1, point 25). It is the latter provision that Decisions 2017 and 2018 refer to as a legal basis for blocking access to web-resources.

At the same time, the Constitution of Ukraine stipulates that the rights and freedoms enshrined therein may not be restricted, except for cases expressly provided for in the constitutional text (Article 64). For freedom of expression, Article 34 strictly outlines restrictions that may be introduced by law. Narrowing of the essence and scope of constitutional rights by law is not allowed (Article 22).

**Therefore, sanctions applied by Decisions 2017 and 2018 do not appear to be in harmony with the applicable constitutional provisions and standards, and might violate the rights of internet providers and internet users alike** because:

- no law in Ukraine provides for blocking access to online services, resources as well as to their subdomains (except for cases of dissemination of child sexual abuse content<sup>14</sup> and cases of violation of copyright and related rights);
- the provision of the law “On Sanctions” underpinning Decisions 2017 and 2018 is formulated in vague terms and allows for broad interpretation, which creates the risk of arbitrary application of measures restricting freedom of expression, including on the internet.

It is worth mentioning that in practice internet providers generally respect decisions of the National Security and Defence Council of Ukraine obliging them to block access to web-resources, even though

---

President of Ukraine “On the Decision of the National Security and Defense Council of Ukraine ‘On application and lifting of individual special economic and other restrictive measures (sanctions)’ of 2 May 2018” of 14 May 2018 No. 126/2018, available at: <https://zakon.rada.gov.ua/laws/show/126/2018>

<sup>13</sup> JSC “Kaspersky Laboratory”, LLC “Kaspersky Laboratory Ukraine”, LLC “Doctor Web”, LLC “Centre for Technic Support “Doctor Web”, LLC “Yandex”, LLC “Yandex.Ukraine”, LLC “Mail.ru Group”, LLC “Mail.ru Ukraine”, LLC “Vkontakte”, LLC “V Kontakte”, WM Transfer Ltd, VMR LLC, WebMoney.Ru LLC, JSC “Non-banking credit organization “Network Clearing House”, JSC “Computational Powers”, WebMoney Europe Ltd, Amstar Holdings Limited, INDX Transactions Ltd, subsidiary company “Financial company EIMi”, WebMoney.ua, subsidiary company “Financial institution “VM-Factor”, Paymaster LLC, LLC Agency of Guaranties, Interselect LLC, Office of Federal State Unitary Enterprise, Representation of the “Russian Information Agency (RIA) “News”, OJSC “Telecompany NTV”, OJSC “First Channel. Worldwide network”, TV channels “RTR-Planet”, channel “Russia-24” (part of the “Wholerussian State Television and Radiobroadcasting Company”), Federal State Unitary Entity “Whole Russian State Television and Radio Broadcasting Company”, OJSC “NTV-Plus”, OJSC “Television and Radio Broadcasting Company of Russian Federation’s Armed Forces “Zvezda”, JSC “TNT-TELEVISION NETWORK”, JSC “MOSCOW MEDIA”, Autonomous non-commercial organization Information center for radio broadcasting, art and culture “VERA, NADEJDA, LIUBOV”, Federal State Unitarian Entity “International information agency “Russia Today”, CJSC “National Media Grup”, JSC “Television and Radio Broadcasting Company “Petersburg”, LLC “Aksept” TV channel “Ren TV”, Autonomous non-commercial organization “Russian Public Broadcasting”, LLC “Media Content”, LLC “Promedia”, LLC “Nashe Radio”, LLC “Media Innovation Group”, LLC “Ukrainian Business Portal”.

<sup>14</sup> Article 39, part 1, point 18 of the Law of Ukraine “On Telecommunications” of 18.11.2003 № 1280-IV, Vidomosty Verkhovnoi Rady of Ukraine, 2004, № 12, Art. 155, available at: <https://zakon2.rada.gov.ua/laws/show/1280-15>

formally such decisions are not binding for private actors.<sup>15</sup> However, research carried out by Digital Security Lab Ukraine in March 2019 (covering 264 web-sites, 70 internet providers in 22 cities of Ukraine, except Kyiv) showed that 20 internet providers have not blocked even a half of the listed resources.<sup>16</sup> Another research by the same company undertaken in May 2019 (covering 264 web-sites and 62 internet providers in 24 cities of Ukraine) showed that the number of providers that have blocked less than a half of prohibited resources has increased to 34.<sup>17</sup>

Another important novelty is the Information Security Doctrine of Ukraine (an act of secondary legislation, adopted by the National Security and Defence Council of Ukraine and further approved and enacted by a Presidential decree).<sup>18</sup> It sets, among other things, the priorities of the State policy of Ukraine in the information sphere. In particular, one of such priorities is regulating the mechanism of identification, blocking and deletion from the State's information space of information that threatens the life or health of Ukrainian citizens, propagates war, national and religious hatred, overthrowing of the constitutional order or violation of national territorial integrity, threatens state sovereignty, propagates communist and/or national-socialist (Nazi) totalitarian regimes and their symbols (chapter 5, part 1, point 4). It further authorises the Ministry of Information Policy of Ukraine to organise and ensure monitoring of mass media and the public domain of the 'Ukrainian segment of the internet' (chapter 6, points 3-5).

After enactment of the Decision 2017 by a Presidential decree, the Ministry of Information Policy undertook preparing its own lists of web-resources that contain 'information prohibited for distribution'. The Information Security Doctrine is considered to have served as a legal basis for this decision.<sup>19</sup> In 2017, a working group set up by the Ministry compiled a list of 20 websites that, in its opinion, contained anti-Ukrainian content and violated Ukrainian legislation prohibiting incitement of inter-ethnic and international hate, calls to overthrow the constitutional order, to infringe territorial integrity, or to violate the legislation on decommunisation. Two additional lists were prepared in 2018 and 2019.<sup>20</sup> All the lists were passed on to the Security Service of Ukraine which, at its turn, sent letters to internet service providers recommending to restrict access to almost all websites from the Ministry's lists (about 60 websites in total).<sup>21</sup>

This approach prompted strong criticism and reactions from the civil society. In 2017 the Ukrainian Internet Association addressed a letter<sup>22</sup> to the Ministry of Information Policy urging it not to pursue this

---

<sup>15</sup> Decisions of the National Security and Defence Council of Ukraine, as enacted by decrees of the President of Ukraine, are legally binding for the executive (Article 10, part 4 of the Law of Ukraine "On National Security and Defence Council of Ukraine" of 05.03.1998 No. 183/98-BP, Vidomosty Verkhovnoi Rady of Ukraine, 1998, № 35, Art.237, available at: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80>)

<sup>16</sup> Available at: <https://bit.ly/2nxAOBK>

<sup>17</sup> Available at: [https://www.facebook.com/cyberlabUkraine/posts/2445347298842108?\\_tn=K-R](https://www.facebook.com/cyberlabUkraine/posts/2445347298842108?_tn=K-R)

<sup>18</sup> Decree of the President of Ukraine No. 47/2017 "On the Decision of the National Security and Defence Council of Ukraine 'On the Information Security Doctrine of Ukraine' of 29 December 2016", available at: <https://zakon.rada.gov.ua/laws/show/47/2017>

<sup>19</sup> "The MIP considers the publication of site blocking criteria a threat to national security", Julia Shestakova, 6 January 2019, Detector Media, available at: <https://detector.media/infospace/article/144054/2019-01-16-mip-vvazhae-oprilyudnennya-kriteriiv-blokuvannya-saitiv-zagrozoyu-natsbezpetsi/>

<sup>20</sup> The Lists of web-sites that contain information that is prohibited by Ukrainian law, available at: <https://mip.gov.ua/en/documents/116.html>

<sup>21</sup> See, for instance, the letter of Security Service of Ukraine to "ЛОАД.МІ" LLC of 25 September 2017 no. 51/9/4-49506, available at: [https://inau.ua/sites/default/files/file/1711/vhidnyy\\_no\\_243\\_vid\\_28.11.2017.pdf](https://inau.ua/sites/default/files/file/1711/vhidnyy_no_243_vid_28.11.2017.pdf)

<sup>22</sup> Letter of the Ukrainian Internet Association to the Deputy Head of Ministry of Information Policy of Ukraine "On the List of internet resources for possible blocking", 21 June 2017 no. 101, available at:

line of action and pointing out the lack of legal basis both for the Ministry and the Security Service to decide on restricting access to internet resources. It further expressed concerns regarding compliance with the principle of net neutrality, stressed the risk of creating a censorship precedent and the risk of opening the door to possible DDoS attacks on critical State infrastructure. It also highlighted that equipment for blocking of concrete web-resources<sup>23</sup> was too expensive for small and the most part of medium-size operators, while by blocking the whole web-site or IP address operators (providers) would violate Ukrainian legislation.

The Ukrainian Internet Association also petitioned to the Security Service reiterating the above concerns and highlighting that restricting access to websites would be in violation of legal requirements on the delivery of services by internet service providers.<sup>24</sup> The Security Service replied that blocking of internet resources by operators and providers of telecommunication services based on its recommendations will not be penalised by virtue of the provision on the “state of necessity” contained in Article 18 of Code of Administrative Offences.<sup>25</sup>

The criteria and methodology used by the Ministry of Information Policy for identifying web-resources included in the lists for blocking were not made public. Whether blocking of internet resources and application of individual special economic and other restrictive measures (sanctions) have proved to be effective, also remains an open question.<sup>26</sup> The Security Service, the Ministry of Foreign Affairs<sup>27</sup> as well as the Ministry of Information Policy<sup>28</sup> do not provide information on this issue arguing that access to it is restricted<sup>29</sup> or that such information belongs to service data.<sup>30</sup>

---

<https://inau.ua/document/lyst-no101-vid-21062017r-zastupnyku-ministra-informacynovi-polityky-ukrayiny-shchodo>

<sup>23</sup> This is about DPI equipment that allows blocking on the basis of URL. Although even in that case it could not prevent blocking of resources that use https protocol.

<sup>24</sup> Letter of the Ukrainian Internet Association to the Head of Security Service of Ukraine “Regarding providing information on the legal grounds for sending letters with recommendations to restrict access of subscribers to certain internet resources”, 8 December 2017 no. 199, available at: <https://inau.ua/document/lyst-no-199-vid-08122017-golovi-sbu-shchodo-nadannya-informaciyi-stosovno-pravovyh-pidstav>

<sup>25</sup> Letter of the Security Service of Ukraine to the Ukrainian Internet Association of 9 January 2018 no. 5/4/2-368, available at: [https://inau.ua/sites/default/files/file/1801/vhidnyy\\_no\\_09\\_vid\\_12.01.2018.pdf](https://inau.ua/sites/default/files/file/1801/vhidnyy_no_09_vid_12.01.2018.pdf)

<sup>26</sup> “The SSU and the Ministry of Foreign Affairs do not disclose information about the effectiveness of internet blocking in Ukraine”, Digital Security Lab Ukraine, 15 May 2019, Medium, available at: <https://bit.ly/2nuJ6yW>

<sup>27</sup> According to the Decision 2017 (part 3) and to the Decision 2018 (part 4, point 1), the Security Service of Ukraine is responsible for monitoring the effectiveness of economic sanctions; according to the Decision 2018 (part 5), the Ministry of Foreign Affairs must inform competent bodies of the European Union, the United States of America and of other States about the sanctions applied invite them to consider applying similar restrictive measures.

<sup>28</sup> The Ministry of Information Policy sends lists of web-sites/resources that disseminate information possibly violating Ukrainian legislation to the Security Service. The Security Service may further propose to the National Security and Defence Council to add such resources to the lists for sanctioning. See “FreeNet Ukraine Coalition will apply to court to require the NSDC, SSU and MIP to reveal the grounds for blocking web-sites”, Platform for Human Rights, available at: <https://www.ppl.org.ua/vimoga-vid-rnbo-sbu-ta-mip-rozkriti-pidstavi-sankcijinogo-blokuvannya-sajtiv.html>

<sup>29</sup> The Security Service of Ukraine confirmed analysing effectiveness of the measures taken, but refused to provide further information because it “was gathered in the course of counterintelligence activity and has restricted access”. See the Letter of the Security Service of Ukraine of 2 May 2019 no. 30/3/2/w-13/r/16/4468, available at [https://drive.google.com/open?id=1PYOho\\_ev6fgN8X99JzIzn64PlfgPhyx-](https://drive.google.com/open?id=1PYOho_ev6fgN8X99JzIzn64PlfgPhyx-)

<sup>30</sup> “The MIP considers the publication of site blocking criteria a threat to national security”, Julia Shestakova, 6 January 2019, Detector Media, available at: <https://detector.media/infospace/article/144054/2019-01-16-mip-vvazhae-oprilyudnennya-kriteriiv-blokuvannya-sajtiv-zagrozoyu-natsbezpetsi/>.

In 2018 the FreeNet Ukraine Coalition – a coalition of civil society groups – initiated two strategic litigation cases against the Ministry of Information Policy, the National Security and Defence Council and the Security Service of Ukraine to provoke public debate and bring transparency to the government’s approach.<sup>31</sup> On 30 September 2019 the court ruled on one of the cases supporting the state authorities’ position that information in question belongs to service data.<sup>32</sup>

Such lack of transparency raises **serious concerns regarding the respect for human rights, in particular – for freedom of expression, and puts into question the availability of safeguards to prevent arbitrariness and abuse of power by public authorities.**

### **2.1.3. Protection of Copyright and Related Rights**

As in 2015, copyright and related rights are regulated by the Civil Code (Chapters 36 - 37) and by the Law “On Copyright and Related Rights” (hereafter – “Law on Copyright”). In March 2017 the Law “On State Support of Cinematography in Ukraine”<sup>33</sup> was adopted, also amending the Law “On Copyright”.

Among other things, camcording and cardsharing were recognised as actions that may violate intellectual property rights and give rise to judicial protection. However, the most important changes were related to the new civil-law remedy against breach of copyright and related rights provided for in Article 52-1 of the Law on Copyright.

Article 52-1 introduced a “notice and take-down” procedure that entitles the victim to file a complaint requesting termination of the violation to the owner of the website and/or of the webpage where relevant content is placed or used. This remedy, however, only applies to the use of audio-visual works, music, computer programs, videograms, phonograms and broadcasts.

Further changes introduced by Article 52-1 include, among others, an obligation for website owners and hosting services providers<sup>34</sup> to publish their identification and contact details; mandatory professional legal support for complaints against copyright/other related rights violations, and a 72 hours deadline for examination of such complaints; a requirement that access to the whole web-resource may only be restricted if limiting access specifically to information referred to in the complaint is not possible. Website or webpage owners that within 48 hours of receiving the complaint have restricted access to the information in question, are absolved of liability (with few exceptions provided for by the Law on Copyright).

Apart from legislative developments, a new practice of blocking web-resources on the basis of orders by investigating judges has emerged in Ukraine recently. Investigators started massively petitioning courts requesting “arrest” of internet users’ “intellectual property rights deriving from the use of web-resources” - by means of obliging internet providers to restrict access to such resources. This practice has originated

---

<sup>31</sup> “To Battle Russian Disinformation, Ukraine Mimics ... Russia”, Samuel Woodhams, 17 April 2019, available at: <https://www.justsecurity.org/63682/to-battle-russian-disinformation-ukraine-mimics-russia/>

<sup>32</sup> [http://reyestr.court.gov.ua/Review/84629889?fbclid=IwAR1K8Inv9mSdk-40jGZNLNd\\_VLuuCo-NFRqY56hSdfBSS6oaj1yMWMLTY-w](http://reyestr.court.gov.ua/Review/84629889?fbclid=IwAR1K8Inv9mSdk-40jGZNLNd_VLuuCo-NFRqY56hSdfBSS6oaj1yMWMLTY-w)

<sup>33</sup> Law of Ukraine “On State Support for Cinematography in Ukraine” of 23.03.2017 No. 1977-VIII, Vidomosty Verkhovnoi Rady of Ukraine, 2017, № 20, Article 240, available at: <https://zakon.rada.gov.ua/laws/show/1977-19#n414>

<sup>34</sup> Except for individuals who do not pursue economic activity and are obliged to publish on their own web-sites or public records’ databases on domain names (WHOIS) contact details of the web-site’s owner and the hosting service provider, including e-mail and telephone number.

from criminal cases connected with drugs dealing<sup>35</sup>, gambling<sup>36</sup>, etc., as there is no law that would expressly allow for blocking of online content in such situations.

However, sometimes such “arrest” requests were sent to courts in connection with online articles containing criticism against state officials. Just as one example in this context, in July 2019 an investigating judge of the Pechersk district court of Kyiv issued an Order requiring some of the biggest Ukrainian internet providers<sup>37</sup> to block whole websites (or their parts in full) - despite the fact that the prosecutor’s petition referred to concrete webpages that allegedly have been used for extortion, dissemination of defamation or other violations.<sup>38</sup>

**The practice of issuing “arrest” orders as a pathway to blocking web-resources appears to be very controversial and raises a number of legal issues, namely:**

- It is highly questionable whether internet users acquire intellectual property rights by accessing and using web-resources. Hence, such grounds for *de facto* blocking of web-sites by court orders appear to be arguable and far-fetched;
- The obligation of internet providers to block web-resources is not provided for by law (except for cases of dissemination of child sexual abuse content);
- Investigators consider internet users’ “intellectual property rights deriving from the use of web-resources” as material evidence, which is in contradiction with the rules on evidence contained in the Criminal Procedural Code;
- And lastly, IP address blocking leads to disproportionate interference with the functioning of web-resources serviced by the same IP, but not involved in the case.<sup>39</sup>

In view of the above, “arrest” orders with regard to intellectual property rights as a means to block web-resources have no clear basis in law and bear serious risks for freedom of expression in Ukraine. Some courts reject requests for such “arrest” orders as not provided for by the Criminal Procedural Code.<sup>40</sup>

#### **2.1.4. Violations in the Sphere of National Security and Public Morals**

Since 2015, there have been no significant changes in law and practice on this issue.

#### **2.1.5. Defamation**

---

<sup>35</sup> See, for instance, notification by the National Commission for the State Regulation of Communications and Informatization, available at: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1746&language=uk>

<sup>36</sup> See, for instance, notification by the National Commission for the State Regulation of Communications and Informatization, available at: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1755&language=uk>

<sup>37</sup> In particular, legal entities through which Vodafone, Triolan, Kyivstar, Lifecell, Volia-Cable, DataGroup, LaNet and others operate. For further information, see notification by National Commission for the State Regulation of Communications and Informatization, available at: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1749&language=uk>

<sup>38</sup> “Owners of the blocked web-sites will appeal”, Vladimir Kondrashov, 5 August 2019, Internetua, available at: <http://internetua.com/sobstvenniki-zablokirovannyh-saitov-budut-osparivat-eto-reshenie-v-sude>

<sup>39</sup> “Attorney: Almost every wording is questionable in the court order blocking a web-site”, Denis Ovcharov, 26 July 2019, Internetua, available at: <http://internetua.com/uarist-v-uhvali-sudu-pro-blokuvannya-saitu-sumnivne-maije-kojne-formuluavannya>

<sup>40</sup> See, for instance, judgment of the Appeal Court of the Mikolaiv Region of 19 January 2018, no. 487/3952/17, available at: <http://reyestr.court.gov.ua/Review/71695380> ; judgment of the Appeal Court of Kyiv of 10 December 2018, available at: <http://reyestr.court.gov.ua/Review/78823865>

There have been no changes in the defamation legislation of Ukraine since 2015. There are still no special legal provisions allowing for blocking of web-resources with regard to dissemination of defamatory content. At the same time, injunctions requesting blocking of web-resources are occasionally used to secure lawsuits in defamation cases.<sup>41</sup> As a general rule, injunctions are to be executed immediately and appeal against them does not preclude the execution.<sup>42</sup> In practice this means that web-resources may remain blocked for the whole duration of court proceedings, which may often be postponed. This carries certain risks for freedom of expression as web-resources may lose their audiences, and also bear losses which eventually result in their closure.

### **2.1.5. Intermediary Liability**

There have been no changes the relevant legislation since 2015. Internet access providers may still be held liable only for a failure to execute a court decision.<sup>43</sup>

However, the enactment of the Decision 2017 by Presidential decree has triggered an immediate reaction from the National Commission for State Regulation of Communications and Informatisation. In its information letter to operators and providers of telecommunications, the Commission stressed that the Decree 2017 was obligatory for execution and reminded that according to Article 75 of the Law “On Telecommunications”, violations of the legislation on telecommunications entail civil, administrative and criminal liability. In addition, the Commission warned operators and providers of telecommunications that in the case of failure to execute the Decree 2017, they may be fined on the ground of Articles 145 and 148-2 of Code of Administrative Offences.<sup>44</sup>

As mentioned before (see section 2.1.2.), formally Decisions 2017 and 2018 are not obligatory for internet providers, although they form part of Ukrainian legislation. Some internet providers execute these Decrees, while others do not. The legal uncertainty of the existing situation is generally not favourable for freedom of expression.

## **2.2. Take-down/Removal of Illegal Internet Content**

### **2.2.1. General Legal Framework**

There have been no changes in the legislation specifically with regard to take-down/removal of illegal internet content since 2015. At the same time, in 2017 the Civil Procedural Code, the Economic Procedural Code and the Code on Administrative Proceedings of Ukraine were entirely revised.<sup>45</sup> In particular, the Economic Procedural Code (Article 5, part 2), as well as the Civil Procedural Code (Article 5, part 2) now provide that where no effective remedy for protection of a violated right or interest exists, courts may apply any remedy that does not contradict the law.<sup>46</sup> It is important to bear in mind that, potentially, application of certain remedies may lead to violation of non-property rights (e.g., take-down/removal of

---

<sup>41</sup> See, for instance, judgment of the Pecherskiyskiy district court of Kyiv of 25 August 2016, available at: <http://www.reyestr.court.gov.ua/Review/59938896>; judgement of the Truskavets city court of 19 April 2018, available at: <http://reyestr.court.gov.ua/Review/73485803>

<sup>42</sup> Civil Procedural Code, Article 153.

<sup>43</sup> Article 18 of Civil Procedural Code, Article 14 of Code of Administrative Proceedings, Article 298 of Code of Ukraine of Administrative Offences, Article 18 of Economic Procedural Code, Article 533 of Criminal Procedural Code.

<sup>44</sup> Information letter for the attention of telecommunication operators and providers, available at: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1237&language=uk>

<sup>45</sup> Law of Ukraine “On Amending of Economic Procedural Code of Ukraine, Civil Procedural Code of Ukraine, Code on Administrative Proceedings of Ukraine and Other Legislative Acts”, Vidomosty Verkhovnoi Rady of Ukraine, 2017, № 48, Article 436, available at: <https://zakon.rada.gov.ua/laws/show/2147-19>

<sup>46</sup> See, for instance, judgment of the Commercial court of the Donetsk region of 4 June 2019, no. 905/405/19, available at: <http://www.reyestr.court.gov.ua/Review/82335661>

a part of an article will interfere with the integrity of the work), or of freedom of expression (e.g., if remedies are applied without due respect for the principle of proportionality as developed in the case-law of the European Court of Human Rights. Therefore prudence and professionalism of the courts will play an important role in forming the practice of implementation of these new provisions.

### 2.2.2. Personal Data Protection

Since 2015 there have been no changes in the legislation of Ukraine on personal data protection. In practice, however, there have been instances of failure to protect personal data.

In particular, massive amounts of journalists' personal data have been leaked into public domain via the "Myrotvorets" website – an online resource of a non-governmental organisation that pursues the aim of *"identifying traitors to Homeland, gunmen, assassins and terrorists, Russian servicemen - war criminals"* [quote from the home page of the "Myrotvorets" website].<sup>47</sup> According to the All-Ukrainian association "Uspishna Varta", the open database available on the "Myrotvorets" website contains personal data that has been collected illegally (e.g., by means of hacking/phishing) as well as from open sources, and published without data subjects' consent."Uspishna Varta" also claims that the Ministry of Internal Affairs, the Security Service and other public authorities remained among the website's partners till May 2016.<sup>48</sup>

In May 2016, a *"List of journalists accredited by the DPR terrorist organization"* [quote from the home page of the "Myrotvorets" website] featuring more than 4000 journalists, including their place of work, mobile phone number, e-mail and the period of stay in the territories of Donetsk and Luhansk regions, appeared on the "Myrotvorets" website.<sup>49</sup> Soon after the list was supplemented with an updated version containing personal data of almost 5500 journalists.<sup>50</sup> Both lists are still freely available online.

Ukrainian and foreign journalists strongly protested against the publication of the lists and called for their take-down.<sup>51</sup> The Ombudsman supported their statement and recommended that the Security Service and the Head of National Police take measures to stop illegal data collection and dissemination and block access to this website in Ukraine.<sup>52</sup> The Committee on Freedom of Expression of the Verkhovna Rada of Ukraine considered the publication unacceptable and in breach of the right to personal data protection, and called on the website and on public authorities to ensure compliance with law.<sup>53</sup> According to

---

<sup>47</sup> <https://psb4ukr.org/about/>, last accessed on 6 April 2020.

<sup>48</sup> "The 'Myrotvorets' web-site and the court practice in Ukraine", Natalya Natalina, 3 September 2018, available at: <https://uspishna-varta.com/ru/novyny/veb-sajt-mirotvorec-i-sudebnaya-praktika-v-ukraine-1>

<sup>49</sup> The list is available at: <https://myrotvorets.center/579804-spisok-zhurnalistov-akkreditovannyx-terroristicheskoy-organizacii-dnr/>, last accessed 6 April 2020.

<sup>50</sup> The updated list is available at <https://psb4ukr.org/587351-izviniya-kollektiva-centra-mirotvorec-po-povodu-publikacii-10-05-2016-spiska-zhurnalistov-akkreditovannyx-terroristicheskoy-organizacii-dnr/>, last accessed 6 April 2020.

<sup>51</sup> Statement "Ukrainian and foreign journalists outraged by the publication of personal information of their colleagues by the 'Myrotvorets' website", 11 May 2016, Detector Media, available at: <https://detector.media/community/article/114995/2016-05-11-ukrainski-ta-inozemni-zhurnalisti-obureni-publikatsiyu-personalnikh-danikh-koleg-saitom-mirotvorets-zayava/>

<sup>52</sup> "Valeria Lutkovskaya insists on the need to take effective measures to stop violations of the right to protection of personal data", 12 May 2016, official website of the Commissioner for Human Rights of the Verkhovna Rada of Ukraine, available at: <http://www.ombudsman.gov.ua/ua/all-news/pr/12516-kb-valeriya-lutkovska-napolyagayena-neobxidnosti-vzhittya-diyevix-zaxodi/>

<sup>53</sup> Statement "The Committee on Freedom of Expression considers publication of journalists' personal data on the 'Myrotvorets' website inadmissible", 12 May 2016, Detector Media, available at: <https://detector.media/infospace/article/115068/2016-05-12-komitet-svobodi-slova-vvazhae-nepripustimipublikatsiyu-personalnikh-danikh-zhurnalistiv-na-saiti-mirotvorets-zayava/>

information from open sources, the Kyiv Prosecutor's office opened a pre-trial investigation based on part 1 of Article 171 of the Criminal Code (obstruction of legal professional journalist activity).<sup>54</sup> No further information on the state of the investigation is available.

Another example is the case of Ukrainian public officials who had obtained Hungarian passports.<sup>55</sup> The "Myrotvorets" website published a list featuring full passport details of more than 300 such public officials from the Transcarpathian region,<sup>56</sup> and two days later updated it adding 200 more names.<sup>57</sup> Both lists remain in public domain up to date.

Despite the fact that "Myrotvorets" is a website of a non-governmental organisation and despite serious data protection issues arising from its activity, courts have accepted information published on the website as evidence for the prosecution in a number of criminal cases.<sup>58</sup>

### 2.2.3. Defamation

As mentioned above (see section 2.2.1.), the revision of three procedural codes in 2017 implies development of new court practice related to take-down/removal of illegal internet content, including defamatory content.

Apart from this, case-law obliging defendants to take down/remove online content started emerging on the basis of legal provisions that already existed before. For instance, in the case of Mr Martynenko (a famous Ukrainian politician and ex-MP) the Pecherskiy district court of Kyiv<sup>59</sup> obliged the "Anti-Corruption Action Centre" (NGO) to take-down/remove information about criminal proceedings involving Mr Martynenko as a suspect from the Public Register of National Public Officials established by this NGO. It also prohibited any further similar publications by the NGO before the final decisions in the respective criminal cases. While the Pechersk district court's decision refers to the Civil Code (Article 296, part 4) which prohibits publishing names of suspects in criminal cases, it appears that the court's approach does not fully take into account the case-law of European Court of Human Rights regarding publication of

---

<sup>54</sup> "The prosecutor's office opened proceedings on the publication of journalists' data by the 'Myrotvorets' website", 11 May 2016, Detector Media, available at: <https://detector.media/infospace/article/115024/2016-05-11-prokuratura-vidkrila-provazhennya-za-faktom-publikatsii-danikh-zhurnalistiv-saitom-mirotvorets/>

<sup>55</sup> According to Ukrainian legislation, double citizenship is not permitted – see Article 4 of the Constitution of Ukraine and the Law of Ukraine "On the Citizenship of Ukraine" of 18.01.2001, No. 2235-III, Vidomosty Verkhovnoi Rady of Ukraine, 2001, № 13, Art. 65, available at: <https://zakon.rada.gov.ua/laws/show/2235-14>

<sup>56</sup> "They swore allegiance to Hungary while working on civil service or in local public authorities of Ukraine", Roman Zaytsev, 8 October 2018, Myrotvorets, available at: <https://myrotvorets.news/ony-prysiahnuly-na-vernost-venhryy-na/>

<sup>57</sup> "At the request of the Hungarian Foreign Ministry, we publish an updated list of Ukrainian officials who swore allegiance to a foreign country", Roman Zaytsev, 10 October 2018, Myrotvorets, available at: <https://myrotvorets.news/po-prosbe-myd-venhryy-publykuem-obno/>

<sup>58</sup> See, for instance, judgment of the Shevchenkovskiy district court of Chernivtsy of 19 January 2018 no. 727/11208/17, available at: <http://reyestr.court.gov.ua/Review/71803897>; judgment of the Lisichanskiy city court of the Lugansk Region of 26 February 2018 no. 415/3619/1, available at: <http://reyestr.court.gov.ua/Review/72688616>; judgment of the Shevchenkovskiy district court of Chernivtsy of 21 June 2016 no. 727/4524/16-к, available at: <http://reyestr.court.gov.ua/Review/58551862>; judgment of the Shevchenkovskiy district court of Chernivtsy of 26 June 2016 no. 727/3812/18, available at: <http://reyestr.court.gov.ua/Review/75006272>; judgment of the Shevchenkovskiy district court of Chernivtsy of 16 March 2018 no. 727/13005/17, available at: <http://reyestr.court.gov.ua/Review/72787331>

<sup>59</sup> Judgment of the Pecherskiy district court of Kyiv of 11 December 2018, no. 757/30830/18-ц, available at: <http://reyestr.court.gov.ua/Review/78556109>

information on matters of public interest (see section 5.4.). Nevertheless, this judgment was later upheld by the Kyiv Appeal Court.<sup>60</sup>

#### **2.2.4. Liability of Internet Host Providers**

As mentioned above, in March 2017 the Law “On Copyright” was amended, including its provisions on the liability of internet hosting service providers. Currently, according to part 1 of Article 52-2 of this Law, hosting service providers have an obligation to include in their terms of service provisions forbidding copyright and other related rights violations by customers. They must also oblige customers to provide their identification and contact details, and ensure that this information is up to date. Compliance with these requirements and with the deadline for blocking of web-resources set in Article 52-2 of the Law “On Copyright” absolves the hosting service provider from liability. Otherwise, the hosting service provider bears responsibility together with the copyright violator.

#### **2.2.5. Safeguards**

In terms of safeguards, the current situation is similar to that of 2015. New concerns about the lack of sufficient safeguards for freedom of expression on the internet arise with regard to adoption and execution of Decrees 2017 and 2018. So far courts have often refused to examine claims about blocked access to web-resources on the grounds that plaintiffs did not have the victim status. Where such cases have been examined on the merits, blocking was considered lawful and proportionate to the aims pursued as internet users were not prevented from accessing other similar internet resources.<sup>61</sup>

### **3. Procedural Aspects**

Apart from the new “notice and take-down” procedure introduced by the Law “On Copyright” (see sections 2.1.3 and 2.1.5), there have been no major changes in the procedural aspects of blocking, filtering and take-down of illegal internet content since 2015.

#### **3.1. Measures on Search of a Housing or Other Dwellings, Temporary Seizure and Arrest of Property**

In February 2016, Article 176 of the Criminal Code was amended so as to make sanctions for violation of copyright and/or related rights less severe, in particular by excluding the sanction of confiscation and destruction of all produce of copyright violation, as well as tools and materials that had been used for production.

Furthermore, in November 2017 Article 168 of the Criminal Procedural Code was amended - temporary seizure of electronic information systems or of their parts, as well as of mobile terminals of communication systems was forbidden. This provision is meant to protect the rights of those involved in the criminal process against arbitrary seizure and arrest of computer equipment. However, the new rule provides for a wide range of exceptions (e.g., where for the purposes of expert examination the device is essential, or where encryption or other protection system needs to be overcome, or where the device is the means or produce of a crime), and for this reason the situation in practice so far remains largely without change.

---

<sup>60</sup> Judgment of the Kyiv Appeal Court of 20 February 2019 no. 757/30830/18-ц, available at: <http://www.apcourtkiev.gov.ua/CourtPortal.WebSite/Home/Sprava/51016924829>

<sup>61</sup> See, for instance, decision of Grand Chamber of the Supreme Court of Ukraine of 5 June 2019 no. П/800/217/17, available at: <http://www.reyestr.court.gov.ua/Review/82738705>

### **3.2. Measures on Taking Down of Internet Content**

Since 2015, there have been no significant changes in law and practice on this issue.

### **3.3. Measures on Delivering of an Order on Obligations**

Since 2015, there have been no significant changes in law and practice on this issue.

#### **3.3.1. Notification Requirements**

Developments since 2015 only concern the new “notice and take-down” procedure introduced by the Law “On Copyright” (see sections 2.1.3 and 2.1.5).

Article 52-1 of the Law on Copyright sets detailed requirements as to the form and contents of the complaint (notification), of the reply to such complaint, as well as of the appeal against a negative reply; the deadlines for submitting and for responding to the complaint; other modalities of the “notice and take-down” procedure.

Special attention must be paid to the potential practical issues that may arise with regard to notification of internet providers about the blocking of web-resources. While at times courts oblige concrete internet providers to block access to web-resources, in a number of cases courts have decided on blocking of web-resources in general - to be implemented by all providers that carry out their activity on the territory of Ukraine and are included in the registry of operators as providers of telecommunications.<sup>62</sup> In such cases, certain providers are not directly notified about the court decision. Even though information about court decisions on blocking is published on the web-site of the National Commission for the State Regulation of Communications and Informatisation, internet providers may not find out in due time about the existence of such a court decision and face intermediary liability.

#### **3.3.2. Safeguards and Legal Remedies**

Since 2015, there have been no significant changes in law and practice on this issue.

## **4. General Monitoring of Internet**

The Information Security Doctrine of Ukraine authorises the Ministry of Information Policy to organise and ensure the monitoring of mass media and the public domain of the “Ukrainian internet segment” with a view of detecting the dissemination of information that violates Ukrainian law, as well as to monitor threats to national interests and national security arising in the information sphere (points 3-5 of Chapter 6). According to the Doctrine, in the course of monitoring the Ministry identifies web-resources that, in its opinion, contain illegal content.<sup>63</sup> As outlined above (see section 2.1.2.), as a result of monitoring, the Ministry puts together lists of web-resources that allegedly contain illegal, which are then passed on to the Security Service.

Besides, on 7 November 2015 the Law “On National Police” entered into force<sup>64</sup> and replaced the Law “On Militia”. According to the new Law, the police performs activities to prevent crime and administrative

---

<sup>62</sup> See, for instance, notifications by the National Commission for the State Regulation of Communications and Informatisation, available at: <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1751&language=uk> and <https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1746&language=uk>

<sup>63</sup> The Lists of web-sites that contain information that is prohibited by Ukrainian law, available at: <https://mip.gov.ua/ru/documents/116.html>

<sup>64</sup> Law of Ukraine “On National Police” of 02.07.2015, No. 580-VIII, Vidomosty Verkhovnoi Rady of Ukraine, 2015, № 40-41, Art. 379, available at: <https://zakon.rada.gov.ua/laws/show/580-19>

offences and takes measures to detect crime and administrative offenses (Article 23, part 1, points 1 and 3). In the sphere of informational and analytical support, the police performs information retrieval and analytic work (Article 25, part 2, point 3). In the internet sphere these functions are performed by the Department of Cyberpolice of the National Police of Ukraine.<sup>65</sup>

## 5. Assessment as to the Case Law of the European Court of Human Rights

In general, the situation remains largely without change from that outlined in the 2015 Comparative Study. At the same time, in view of the new developments related to adoption of the Decrees 2017 and 2018 it could be argued that relevant legislation and practice do not fully comply with the standards developed in the case law of the European Court of Human Right. Some provisions of Ukraine's new procedural codes also raise certain concerns as regards alignment with such standards.

### 5.1 Protection of Copyright and Related Rights

The new "notice and take-down" procedure introduced in the Law "On Copyright" generally appears to be in line with Council of Europe standards, in particular with the Committee of Ministers Recommendation (2018)2 on the roles and responsibilities of internet intermediaries. It however still needs to pass the time test to prove its efficiency.

At the same time, the newly emerged practice of "arrest" of internet users' "intellectual property rights deriving from the use of web-resources" on the basis of orders by investigating judges obliging internet providers to restrict access to online resources (see section 2.1.3.) is worrying. While such arrest orders clearly create interference with the right to freely receive and impart information and ideas, their legal basis is questionable. Some courts reject requests for such "arrest" orders as not provided for by the Criminal Procedural Code. Unfortunately, however, this precarious practice generally keeps spreading.

Apart from questionable compliance of this practice with the criterion of legality, where access is restricted to whole websites and not just to the content in question, the issue of proportionality of interference arises.<sup>66</sup>

### 5.2. Legislation in Spheres of National Security and Public Morals

As mentioned in section 2.1.2., the Decrees 2017 and 2018 obliged internet providers to block certain internet resources, as well as their subdomains, even though this type of sanction is not expressly provided for by law. Therefore, the application of these sanctions appears to be in breach of the principle of legal certainty due to the lack of foreseeability.<sup>67</sup>

Besides, where access is blocked to the whole web-resources and not just to illegal content, compliance with the principle of proportionality is at issue. In a similar situation in the case of *Ahmet Yildirim v. Turkey*<sup>68</sup> the European Court of Human Right found a violation of Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention").

---

<sup>65</sup> Official website: <https://cyberpolice.gov.ua/contacts/>

<sup>66</sup> See, for instance, *Ahmet Yildirim v. Turkey*, no. 3111/10 , 18 December 2012

<sup>67</sup> See, for instance, *Sunday Times v. the United Kingdom*, no. 6538/7426, April 1979, *Rotaru v. Romania*, no. 28341/95, 4 May 2000.

<sup>68</sup> *Ahmet Yildirim v. Turkey*, no. 3111/10 , 18 December 2012.

### **5.3. Defamation Cases**

While nothing has changed in the defamation legislation as such, amendments to the Economic Procedural Code and the Civil Procedural Code (see section 2.2.1.) prompt development of new court practice, which also involves take-down/removal of allegedly defamatory content. As the law now leaves the choice of remedy for protection of violated rights to courts in cases where no such remedy is expressly provided for by law or by contract between the parties involved, conformity of the newly developing court practice with the principles deriving from the case law of the European Court of Human Right largely depends on prudence and professionalism of judges.

It is of crucial importance that before ordering content take-down/removal, domestic courts carry out a thorough assessment of all relevant circumstances of the case (e.g., distinguish between facts and value judgments, examine whether the statement at issue constitutes a matter of public interest, take into account the status of the parties involved bearing in mind that the limits of acceptable criticism are wider with regard to politicians and other public figures).<sup>69</sup> Due attention must be paid to proportionality of the measures applied and their necessity in a democratic society.<sup>70</sup>

This is equally valid for court practice on take-down/removal of allegedly defamatory content that has legal basis in legal provisions other than the revised Procedural Codes (e.g., such as in the case of Mr Martynenko – see section 2.2.3.).

### **5.4. Personal Data Protection**

While the assessment of the state of law on personal data protection in Ukraine made in the 2015 Comparative study still stands, it appears to be a worrying sign that in practice large amounts of personal data collected and published without consent of data subjects remain in public domain for a considerable period of time (see section 2.2.2.). It shall be borne in mind in this context that tolerance of the State to acts that carry serious risks to the safety of journalists and other media actors may result in a chilling effect on freedom of expression. According to the case law of the European Court of Human Rights, States are required to create a favourable environment for participation in public debate by all the persons concerned, enabling them to express their opinions and ideas without fear.<sup>71</sup>

It is also worth mentioning that while Ukraine is party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, up to date it has not signed the Amending Protocol<sup>72</sup> aimed at reinforcing protection for individuals in the digital era.

#### **5.4.1. Self-regulatory Frameworks**

There have been no changes in this part since 2015.

#### **5.4.2. Safeguards and Implementation of Legal Requirements**

There have been no changes in this part since 2015.

---

<sup>69</sup> See, for instance, *Lingens v. Austria*, no. 9815/82, 8 July 1986.

<sup>70</sup> See, for instance, *Ahmet Yildirim v. Turkey*, no. 3111/10, 18 December 2012.

<sup>71</sup> *Dink v. Turkey*, nos. 2668/07 6102/08 30079/08 7072/09 7124/09, 14 September 2010, § 137

<sup>72</sup> Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS.223, open for signature by the Contracting States to Treaty ETS 108 in Strasbourg on 10 October 2018.