ARTICLE 19

Russia: The "Right To Be Forgotten" Bill

August 2015

Legal analysis

Executive summary

In August 2015, ARTICLE 19 analysed the so-called "Right To Be Forgotten" Bill of the Russian Federation ('the Bill'), which was signed into law in July 2015 and will come into force on 1 January 2016.

When introducing the Bill, Russian lawmakers referred to the 2014 ruling of the Court of Justice of the European Union (CJEU) in the *Google Spain* case, arguing that Russian citizens should also enjoy a "right to be forgotten." The Bill gives Russian citizens the right to request that search engines remove links about them that are in violation of Russian law, inaccurate, out of date, or irrelevant because of subsequent events or actions taken by the citizens.

In this legal analysis, ARTICLE 19 examines the compatibility of the Bill with international standards on freedom of expression. We find that, while the Bill broadly seeks to replicate the more limited right that was recognised by the CJEU in the *Google Spain* case, it fails to provide the crucial safeguards for the protection of the right to freedom of expression that the CJEU had identified. In particular, Russian lawmakers have failed to carve out limitations on "right to be forgotten" when the personal information at issue is in the public interest and/or concerns public figures.

Important procedural safeguards are also missing, including the right of linked-to sites to be notified that a "right to be forgotten" request has been made in respect of their content and a requirement that search engines publish transparency reports containing sufficiently detailed information about the nature, volume and outcome of "right to be forgotten" requests. Moreover, search engines are required by the Bill to take action in relation to the Internet, i.e. all domain names, rather than .ru domains names.

ARTICLE 19 calls on the Russian Government to urgently review the Bill and ensure that its provisions comply with international human rights standards on freedom of expression.

Key recommendations:

- The new Article 110 of Federal Law no. 149-FZ On Information, Information Technologies and Data Protection included in the Bill should be entitled "right to request the delisting of search results on the basis of a person's name;"
- The applicability of the Bill should be subject to the operator having a branch or subsidiary established in the Russian Federation;
- The material effect of a successful "right to be forgotten" request should be limited to de-listing search results generated on the basis of a search for a person's name;
- Any "right to be forgotten" provision should, at the very least:
  - contain an overarching presumption that information already legitimately in the public domain should remain in the public domain save where it has demonstrably caused serious harm to the person concerned;
  - a broad exception for personal information in the public interest and personal information concerning public figures.
- More generally, any law granting a "right to be forgotten" should provide for balancing exercise with the right to freedom of expression, and if appropriate, set out a non-exhaustive list of indicative criteria to be taken into account when carrying out that balancing exercise.
- The scope of a successful "right to be forgotten" request should be strictly limited to .ru domains.

- The Bill should provide a right for linked-to sites to be notified and at the very least give them an opportunity to intervene in cases being challenged by search engines before the courts.
- The Bill should require that search engines publish sufficiently detailed information about the nature, volume, and outcome of de-listing requests.

Table of contents

Introduction **5**

Relevant international standards on freedom of expression and privacy **6**

Right to freedom of expression 6

The right to privacy and its relationship with the right to freedom of expression 7

Data protection 8

"The right to be forgotten" 10

Analysis of the Bill **11**

Definitions 11

Duties of a search engine operator 13

General remarks 13

The legal test for defining whether search results should be delisted is unduly broad 14

The type of action required from companies is unclear and disproportionate in scope 16

"Right to be forgotten" procedure 16

About ARTICLE 19 ..... **18**

Introduction

On 14 July 2015, the Russian President, Vladimir Putin, signed the so-called "Right To Be Forgotten" Bill into law (the Bill).[1] In introducing the Bill, Russian lawmakers referred to the ruling of the Court of Justice of the European Union (CJEU) in the *Google Spain* case, arguing that Russian citizens should also enjoy a "right to be forgotten."[2] The Bill gives Russian citizens a right to request the de-listing of links about them that are in violation of Russian law, inaccurate, out of date, or irrelevant because of subsequent events or actions taken by the citizens. The Bill will come into force on 1 January 2016.

In this legal analysis, ARTICLE 19 examines the compatibility of the Bill with international standards on freedom of expression. While the Bill broadly seeks to replicate the more limited right that was recognised by the CJEU in the *Google Spain* case, it fails to provide many crucial safeguards for the protection of the right to freedom of expression also identified by the CJEU in that ruling. In particular, Russian lawmakers have failed to establish limitations to the so-called "right to be forgotten" where the personal information at issue is in the public interest and/or concerns public figures. Important procedural safeguards are also missing, including the right of linked-to sites to be notified that a "right to be forgotten" request has been made in respect of their content and a requirement that search engines publish transparency reports containing sufficiently detailed information about the nature, volume, and outcome of "right to be forgotten" requests. Moreover, search engines are required to take action in relation to the Internet, i.e. all domain names, rather than only .ru domains names.

Whilst the new Bill does not contain any sanctions for non-compliance at this stage, the Russian Duma is likely to consider new legislative proposals in the coming months that would impose an administrative fine in circumstances where a search engine fails to de-list the links related to a data subject's personal information upon his or her request, or fails to comply with a court decision requiring the delisting of such links. ARTICLE 19 will closely monitor upcoming parliamentary debates on this issue and stands ready to provide further advice on the implications of the "right to be forgotten" for freedom of expression in Russia.

This legal analysis is divided into two parts. First, we set out the relevant international standards on the rights to freedom of expression, privacy and data protection that are applicable to the subject. Second, we analyse the Bill in detail and provide recommendations on respective issues.

ARTICLE 19 hopes that the analysis will contribute to a better understanding by policy-makers, search engines, and the courts of the proper balance between the right to freedom of expression and the so-called "right to be forgotten." We also urge Russian legislators to consider these recommendations during revision of the Bill.

---

[1] The Bill introduces amendments to the Federal Law On information, information technologies, and data protection and Articles 29 and 402 of the Civil Procedure Code. ARTICLE 19's analysis is based on an unofficial English translation of the Law. We do not take responsibility for the accuracy of the translation or for comments made on the basis of any inaccuracies in the translation.

[2] See e.g. Russia and India Report, *New 'Right to be Forgotten' Law Stirs Controversy*, 15 July 2015.

Relevant international standards on freedom of expression and privacy

Right to freedom of expression

Freedom of expression protects the free flow of information, opinion and ideas. It applies to all media and without regard to borders. It includes the right not only to impart but also to seek and receive information.[3] Freedom of expression has long been recognised as fundamental to both individual autonomy and a free society in general. [4]

The right to freedom of expression is recognized in the Russian Federation's Constitution[5] and in most international human rights treaties to which the Russian Federation is a state party. In particular, it is guaranteed by Article 19 of the **Universal Declaration of Human Rights** (UDHR), Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR) and Article 10 of the **European Convention on Human Rights** (ECHR).[6]

In **General Comment No 34**, the UN Human Rights Committee (HR Committee), the treaty body responsible for the progressive interpretation of the ICCPR, confirmed that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[7]

Freedom of expression is not absolute, however. In particular, Article 19 ICCPR and Article 10 ECHR make clear that freedom of expression is a qualified right. This means that expression may be limited provided the restriction complies with a three-part test:
The restriction must:

- be provided by law;
- pursue one or more of the legitimate aims explicitly enumerated under international law; and
- be necessary in a democratic society. In particular, the requirement of necessity entails that the measure adopted must be proportionate to the aim pursued. If a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure must be applied.

---

[3] This right is contained in Article 19 of the Universal Declaration on Human Rights 1948; Article 19 of the ICCPR 1966; Article 10 of the ECHR 1950; Article 13 of the American Convention on Human Rights 1969; Article 9 of the African Charter on Human and Peoples' Rights.

[4] See, e.g. European Court, *Handyside v the UK*, no. 5493/72, para. 49, 7 December 1976.

[5] Article 29.

[6] The UDHR, as a UN General Assembly Resolution, is not directly binding on states. However, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law since its adoption in 1948. Moreover, the Russian Federation ratified the ICCPR on 16 October 1973 and the ECHR on 05 May 1998. It is therefore legally bound to ensure and respect the right to freedom of expression as contained in Article 19 ICCPR and Article 10 ECHR.

[7] UN Human Rights Committee General Comment No.34, para. 12.

International law therefore allows freedom of expression to be subjected to certain restrictions for the sake of legitimate interests including the rights of others.

The right to privacy and its relationship with the right to freedom of expression

Privacy is a broad concept relating to the protection of individual autonomy and the relationship between an individual and society, including government, companies, and private individuals.[8] It is often summarized as 'the right to be left alone' but encompasses a wide range of rights including protections, from intrusions into family and home life to communications secrecy.[9] It is commonly recognized as a core right that underpins human dignity and other values such as the freedom of association and freedom of speech.[10]

The legal right to privacy is recognized in the Russian Federation's Constitution[11] and in most international human rights treaties to which the Russian Federation is a state party. In particular, it is guaranteed by Article 12 UDHR, Article 17 ICCPR, and Article 8 ECHR. The right to privacy is legally protected in a number of ways at the national level in nearly every country in the world. Most nations have civil and often criminal code protections of this right.[12]

The relationship between the right to privacy and the right to freedom of expression is a complex one. On the one hand, the protection of the right to privacy in online communications is essential for ensuring that individuals have the confidence to freely exercise their right to freedom of expression.[13] The publication of private information constitutes a clear infringement of the right to privacy. Like the right to freedom expression, the right to privacy is not absolute and is subject to the three-part test: legality, necessity and proportionality.[14] Among other things, this means that States, when passing measures to protect the right to privacy, are required not to unduly restrict the right to freedom of expression, such as a requirement on newspapers to notify the subjects of a news article before its publication.[15]

In other words, freedom of expression and the right to privacy are mutually reinforcing but also, paradoxically, conflicting rights. In the seminal case of *Von Hannover v. Germany (No. 2)*, the European Court of Human Rights (European Court) clarified that when balancing the right to

---

[8] See David Banisar, The Right to Information and Privacy: Balancing Rights and Managing Conflicts, World Bank Institute, Governance Working Paper Series, 2011.

[9] The European Court of Human Rights noted that "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. *Niemietz v. Germany*, 16 December 1992, 16 EHRR 97. For a detailed overview of the different rights, see Privacy and Human Rights EPIC and Privacy International, 2006.

[10] See e.g. HR Committee, CCPR General Comment No. 16 on Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988; Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/37, 28 December 2009; *Bensaid v United Kingdom* 44599/98 [2001] ECHR 82.

[11] Articles 23 to 25.

[12] US Department of State, 2010 Human Rights Report; Privacy and Human Rights 2006 (EPIC and Privacy International); Glasser (ed.), International Libel and Privacy Handbook (Bloomberg, 2006).

[13] See UN Special Rapporteur, A/HRC/23/40, at paras. 24-27.

[14] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009; see also Article 8 ECHR.

[15] European Court, *Mosley v the United Kingdom,* no. 48009/08, 10 May 2011.

freedom of expression and the right to privacy, as a matter of principle, both rights deserved *equal respect*.[16] The Court went on to identify a number of relevant factors in balancing these rights, including:

- the contribution to a debate of public interest;
- how well-known the person concerned is and the subject of the report;
- the prior conduct of the person concerned;
- content, form, and consequences of the publication;
- circumstances in which photos were taken (where applicable).

With the rise of data protection law, however, the balance between the right to freedom of expression and the right to privacy has taken on a new dimension and additional factors may therefore have to be taken into account.

Data protection

In the information age, the right to privacy has evolved to address issues relating to the collection, use, and dissemination of personal information in information systems. New technologies have driven the collection of personal information by governments and private bodies in unprecedented vast databases. Governments and private organizations collect information related to government services and obligations, including tax, medical, employment, criminal records, and citizenship. Technologies for identification, including identity card systems, fingerprints, and DNA, have quickly evolved and expanded.

Starting in the 1960s, principles governing the collection and handling of this information known as "fair information practices," were developed and adopted by national governments and international bodies.[17] The principles generally are as follows:

- **Collection Limitation Principle**. There should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and/or consent of the data subject.

- **Data Quality Principle**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

- **Purpose Specification Principle**. The purposes for which personal data are collected should be specified at the time of data collection. Subsequent use of data should be limited to the fulfilment of those purposes or of other purposes compatible with the specified purposes or revised specified purposes.

- **Use Limitation Principle**. Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified above except: a) with the consent of the data subject; or b) by the authority of law.

---

[16] European Court, *Von Hannover v. Germany No.2,* [GC], Nos. 40660/08&60641/08, para. 106, 2012.

[17] OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data (1980); see also US Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems July, 1973; Canadian Standards Association (CSA) International, Model Code for the Protection of Personal Information, 1996.

- **Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification, or disclosure.

- **Openness Principle**. There should be a general policy of openness about developments, practices, and policies with respect to personal data. There should be readily available means for establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle**. An individual should have the right:
  - to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;
  - to obtain such data within a reasonable time;
  - to obtain data at a charge, if any, that is not excessive;
  - to obtain data in a reasonable manner; and
  - to obtain data in a form that is intelligible to him or her;
  - to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
  - to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

- **Accountability Principle**. A data controller should be accountable for complying with measures that give effect to the principles stated above.

In Europe, both the Council of Europe[18] and the European Union[19] have incorporated these principles into data protection treaties. Of these international instruments, the EU Data Protection Directive has been the most influential: it has been adopted by the 28 EU member states, and has been used as a model for the data protection framework of numerous other countries in Europe, Africa, and Latin America that trade with the EU. Moreover, Article 8 of the EU Charter of Fundamental Rights expressly protects the right to the protection of personal data and Article 24 (1) of the Russian Constitution broadly protects the collection, storage, use, and dissemination of information about the private life of a person.

The protection of personal data has become especially important as information service providers such as search engines or social media platforms have become ubiquitous in our daily lives. The development of data protection law to protect personal information held primarily in electronic form has become a fundamental aspect of the way in which we protect our right to privacy in the digital age.

The rise of data protection law also raises significant issues for the protection of freedom of expression online, particularly when it is interpreted as providing a form of the 'right to be forgotten online' without adequate safeguards on the public's right to seek and receive information.[20] This is especially so given that data protection protects 'personal' information, i.e. information which may be both private and public. In practice, this means that conflicts

[18] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, ETS 108, 1981.
[19] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050, 24 October 1995.
[20] Case C-131/12, *Google Spain v. AEPD and Mario Costeja Gonzalez*, 13 May 2014.

between the different rights involved may be especially difficult to manage when the information at issue is both personal and public.

"The right to be forgotten"

The "right to be forgotten" is not recognised as such in international human rights instruments or national constitutions. Rather, a number of domestic and supranational courts have derived it from data protection law,[21] personality rights,[22] defamation law, and/or the right to control one's image.[23] Nonetheless, for the purposes of human rights treaties, this means that the "right to be forgotten" should be considered under the right to privacy and/or the right to protection of personal data.

The "right to be forgotten" is a misnomer, as the "right" may take on different forms. In the EU, for instance, the CJEU has recognised the **right of individuals to request the de-listing of search results generated by a search made for their name**. In practice, this means that the information remains available and may be found using different search terms. At the same time, domestic courts and parliaments could adopt a broader right of erasure so that the information would no longer be available, regardless of the search terms being used.

Since the contours of the 'right to be forgotten' remain relatively under-developed, it is worth examining in more detail the CJEU's judgement in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (Google Spain). As noted above, the CJEU held that data subjects had a right to request Google and other search engines operating in the EU to de-list links to results generated by a search for their name. The CJEU found:

> 81. As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, … that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.

The CJEU therefore introduced a limited counter-balancing exercise for the protection of freedom of expression.[24] As the CJEU was applying data protection law principles, the key test to be applied in "right to be forgotten" cases is whether the personal information at issue is "inadequate, irrelevant, or no longer relevant."

---

[21] *Ibid.*

[22] See Matthew Dougherty, *Japan: Google Privacy Case*, DLA Piper blog, 17 October 2014.

[23] See Global Voices Online, *Right to be forgotten: a Win for Argentina's Lawsuit Happy Celebrities?* 18 September 2014.

[24] For more information, see ARTICLE 19, *A right to be forgotten? EU Court sets worrying precedent for free speech*, 14 May 2014.

Since then, both the Article 29 Working Party and Google's Advisory Council have published guidelines on the way in which "right to be forgotten" requests should be treated.[25] Moreover, several domestic courts within the EU have handed down judgments on the topic, highlighting the importance of protecting the right to freedom of expression.[26]

Analysis of the Bill

The Bill introduces amendments to existing Federal Law No 149-FЗО 'On Information, Information Technologies and Data Protection' and to articles 29 and 402 of the Civil Procedural Code of the Russian Federation.

The Bill sets out the following general procedure for citizens to exercise the "right to be forgotten":

- a claimant has a right to apply with a request, to the search engine operators in question, that they de-list information about them, on the grounds that he or she believes to be valid in line with the Russian law;
- The applicant's claim must include specific information, which the search engines subsequently verify. If the information is found to be incomplete, the search engine operators *have the right* to ask the claimant to add particular missing pieces of information to the initial request.

It appears to be unclear, however, whether the operators are actually exonerated from the responsibility to undertake any actions in cases where the original claim is found incomplete.

Nevertheless, should the applicant receive a request to complement the initial claim, he or she is obliged within 10 working days period to update it and send it back to the search operators, who, in turn, within the same time period must either accept the claim, or reject it and subsequently notify the applicant. If the claimant considers the rejection unfounded, he or she has a right to challenge this in court. It is worth noting that the Bill obliges the search engines not to disclose any information whatsoever regarding the claim.

Definitions

Article 1(1) of the Bill defines "search engines" for the purpose of the existing Federal Law no. 149-FZ on information, information technologies, and data protection. It defines a search engine as:

> [A]n information system which searches for information with a certain content on the Internet network at a user's request, and provides the user with the links to website pages on the Internet network allowing access to the requested data, which is stored on the Internet

[25] See The Article 29 Working Party Guidelines, 26 November 2014; the Report of Google's Advisory Council, 6 February 2015.

[26] See e.g. Court of Amsterdam decision, C/13/569654, 18 September 2014; *Rechtbank Amsterdam,* 13 February 2015, [eiser] tegen Google Inc., *ECLI:NL:RBAMS:2015:716 (Amsterdam Court, 13 February 2015, [plaintiff] v. Google Inc., ECLI:NL:RBAMS:2015:716)*; TGI de Toulouse (ord. réf.), 21 January 2015 - *Franck J. c/ Google France et Google Inc. (Regional court of Toulouse (under the urgent procedure),* 21 January 2015 - *Franck J. v. Google France and Google Inc.).*

> websites belonging to other persons, save for the information systems used for the performance of state and municipal functions, provision of state and municipal services and implementation of other public powers established by the federal laws.

ARTICLE 19 notes that there is no universally agreed definition of "search engines" for the purposes of regulation, for instance:

- The OECD does not define "search engines" but notes that they are one of several Internet intermediaries, which are defined as "bringing together or facilitating transactions between third parties on the Internet. [Internet intermediaries] give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet- based services to third parties."[27]

- There is no agreed definition of search engines under EU law that is relevant from a comparative perspective. Rather, the various activities of information society providers, including search engines, should be considered under both the E-Commerce Directive (ECD) and the Data Protection Directive.
  - Under the ECD, search engines are merely described as "information society services."[28] In practice, the liability of search engines has been determined by reference to the various *activities* listed under the ECD, namely "mere conduit," "caching" and "hosting."[29] Whether or not search engines activities amount to "mere conduit" or "hosting" has been determined differently across the various EU member states.

  - Following the CJEU's judgement in *Google Spain*, search engines have also been categorised as "data controllers" for the purposes of the EU Data Protection Directive.[30] In particular, the CJEU found that "the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as the "processing of personal data" (…) *when that information contains personal data* and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing." [emphasis added]

- Finally, it is worth noting that courts in several common law countries have found that search engines such as Google should not be considered as "publishers" for the purposes of defamation law as the generation of search results is an automated process in which search engines play a primarily passive role.[31] In the UK, for instance, Justice Eady noted

---

[27] OECD, *The Economic and Social Role of Internet Intermediaries*, 2010.

[28] Recital 18 of the E-Commerce Directive 2000.

[29] Articles 12-14 ECD.

[30] *Google Spain*, *op.cit.*, para. 41.

[31] See the recent Canadian decision in *Niemela v Google* (2015 BCSC 1024) applying the Supreme Court of Canada's decision in *Crookes v. Newton*, 2011 SCC 47; see also *Bleyer v. Google Inc.* [2014] NSWSC 897; for a review of recent case law on these issues, see Inforrm, Case Law Canada: Niemela v. Google Inc, British Columbia Court dismisses claim for worldwide libel injunction against Google – Hugh Tomlinson QC, Sara Mansoori, 24 July 2015.

that search engines *automatically* compile and update an index of pages from the web and that search engines such as Google have no control over the search terms entered by users of the search engine or of the material which is placed on the web by its users.[32] Justice Eady therefore concluded that search engines could not be regarded as publishers of third-party content.

While the above list is far from exhaustive, it is not reflected in the definition under the Bill. In our view, the proposed definition of search engines under the Bill is unclear for the following reasons:

- The definition seems to conflate:
  - the activities of search engines, consisting of indexing and making available *information* published or placed on webpages by third parties, vis-à-vis the search engine;
  - the activities of websites, which may both publish their own content and/or host content published by third parties;
  - the kind of information published on webpages which may or may not include *personal information* about third-parties vis-à-vis the publisher.

- Moreover, the definition seems to give exemption to personal information held or published by public authorities. This appears to be at odds with a core principle of data protection law - that individuals are entitled to request the erasure of material published by public authorities that they consider to be inaccurate, irrelevant, or excessive. There should be a presumption that information published by public bodies should remain in the public domain.

Recommendation:

- At the minimum, the words "which is stored on the Internet websites belonging to other persons, save for the information systems used for the performance of state and municipal functions, provision of state and municipal services, and implementation of other public powers established by the federal laws" should be removed.

Duties of a search engine operator

General remarks

- **Title**: Article 1(2) of the Bill adds a new Article 110 to Federal Law no. 149-FZ On Information, Information Technologies and Data Protection. In particular, it sets out "the duties of a search engine operator." At the outset, ARTICLE 19 notes that the title of this provision is unhelpful as it suggests that search engines owe a duty of care to third parties in the provision of their services. In our view, this is inconsistent with international standards on freedom of expression, which provide that intermediaries, including search engines, must benefit from broad liability exemptions for third party content. In our view, it would be preferable for this section to be entitled 'right to request the de-listing of search results on the basis of a person's name'.

[32] See Metropolitan International Schools Limited brought a defamation case against Designtechnica Corporation, Google UK Limited, and Google Inc [2011] WLR 1743, paras 9-13.

- **Applicability:** ARTICLE 19 notes that the Bill is particularly far-reaching since it will apply to any search operator "who places advertisements on the Internet network aimed at attracting the attention of consumers located on the territory of the Russian Federation". The Bill is therefore clearly intended to apply beyond Russian search engines to Google and other search engine operators who are based – and may collect the personal data of Russian nationals from - outside the Russian Federation.

  This provision also seems to suggest that the Bill would apply regardless of the establishment of a subsidiary or a branch of the operator on the territory of the Russian Federation. It therefore seems to go beyond the findings of the CJEU in *Google Spain,* which held that the "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State." In other words, it appears that a search engine operator would be subject to the Bill even if it does not have a subsidiary on the territory of that country, as long as adverts appear in Russian or are otherwise ostensibly aimed at Russian consumers. At a minimum, in our view, the applicability of the "duties of a search engine operator" should be subject to the operator having a branch or subsidiary established in the Russian Federation.

Recommendations:

- The new Article 110 of Federal Law no. 149-FZ On Information, Information Technologies and Data Protection included in the Bill should be entitled "right to request the delisting of search results on the basis of a person's name;"
- The applicability of the Bill should be subject to the operator having a branch or subsidiary established in the Russian Federation.

The legal test for defining whether search results should be de-listed is unduly broad

New Article 110 (1) of Federal Law no. 149-FZ On Information, Information Technologies and Data Protection provides that search engine operators falling within the scope of the law must "stop providing links to the website pages on the Internet network allowing access to information about an applicant which is distributed in violation of the legislation of the Russian Federation, is inaccurate and dated, [or] which has lost meaning for the application by virtue of any subsequent events or actions taken by the applicant."

Article 110 (1) further provides that information about events containing elements of criminally punishable acts in respect of which the periods of limitation for bringing a prosecution have not expired, or information about citizens having committed an offence in respect of which the conviction has not been quashed or been removed from official records, should not be delisted.

ARTICLE 19 notes that the above provision is broadly similar to the so-called 'right to be forgotten', which was recently recognised in the *Google Spain* judgment:

- It puts search engines in the position of having to determine whether personal information is 'inaccurate, dated, or no longer relevant' in light of subsequent events involving the applicant;

- The legal test to be applied when considering "right to be forgotten" applications is broadly equivalent to the 'inadequate, irrelevant or no longer relevant' test in the *Google Spain* judgement.

To this extent, the provision of the Bill shares many of the shortfalls we identified in our response to Google's call for comments on the "right to be forgotten," namely:[33]

- Whether personal information is 'relevant' is an unduly broad measure against which to decide whether information should remain genuinely accessible. In particular, it assumes that personal information is only relevant in the eye of the person making the "right to be forgotten" application. However, information about a person may be both personal and public - it may be relevant to the person seeking the information, and may be relevant insofar as it concerns a matter of public interest. In other words, there is no such thing as an *objective* conception of relevance. In requiring search engines to determine the 'relevance' of information, lawmakers and courts set an impossible task.

- It puts private operators in the position of having to decide matters, involving a complex balance between the rights to privacy, data protection, and freedom of expression. These should be properly determined by the courts or at the very least by an independent adjudicatory body.

Moreover, the scope of the "right to be forgotten" under the new Article 110 (1) is much broader than that recognised by the CJEU and fails to provide sufficient safeguards for the right to freedom of expression:

- The new Article 110 entirely fails to make reference to the right to freedom of expression as an important right which must be balanced with the right to privacy and/ protection of personal data during the examination of "right to be forgotten" requests. Indeed, freedom of expression is not even mentioned in the Bill.

- Although the fact that search engines are not required to de-list links concerning allegations of criminality or information about convictions, which have not been expunged or quashed, is a positive step, this exception is unduly narrow. Instead, Russian law should provide for a much broader exception for personal information in the public interest. In particular, as a matter of principle, the right to request the delisting of links should not be applicable in respect of: (i) personal information, which is already public, save where the availability of that information has caused serious harm to the person concerned; (ii) personal information which is in the public interest; (iii) personal information concerning a public figure.

- We further note that the Bill requires search operators to stop providing links to information about a person that has been disseminated in violation of Russian law; however, it does not specify the relevant Russian laws at issue. In practice, this means that, in the absence of a public interest exception, search operators could be required to de-list links to material that has been obtained unlawfully but which nonetheless has public interest value. For instance, important information in the public interest (e.g. links to documents released by whistleblowers) could be delisted in response to a "right to be forgotten" request if the names of military commanders are mentioned in those documents. Moreover, if the laws in

[33] See ARTICLE 19's Response to Google Advisory Council, October 2014.

question are unduly broad, there is a risk that access to vast swathes of legitimate information may be prevented.

Recommendation

- Any "right to be forgotten" provision should, at the very least:
  - contain an overarching presumption that information already legitimately in the public domain should remain in the public domain save where it has demonstrably caused serious harm to the person concerned;
  - a broad exception for personal information in the public interest and personal information concerning public figures.
- More generally, any law granting a "right to be forgotten" should provide for balancing exercise with the right to freedom of expression, and if appropriate, set out a non-exhaustive list of indicative criteria to be taken into account when carrying out that balancing exercise.

The type of action required from companies is unclear and disproportionate in scope

ARTICLE 19 further notes that the action required by the search engine is unclear. In particular, it is unclear whether search engines are required to remove the links at issue entirely or whether they must de-list search results generated on the basis of a person's name. In Article 10.3., paragraph one suggests that search engines are required to remove links entirely, while paragraphs 2 and 5 suggest that links should be de-listed in response to searches made on the basis of the applicant's name.

In our view, the former would be much more problematic as it would entirely prevent access to information that is considered 'irrelevant' but may otherwise be perfectly legitimate. Any law providing for a "right to be forgotten" should be limited to a right to de-list search results generated on the basis of a search for a person's name.

Furthermore, we note that, provided that a "right to be forgotten" request meets the various criteria set out in the Bill, search engines are required to stop providing links to website pages 'on the Internet network'. In other words, the Bill requires search engines to delist search results from all domain names, not just .ru. In our view, extending the scope of the Bill beyond Russian domain names is grossly disproportionate, as information considered unlawful under the Bill may well be perfectly lawful in other countries; particularly those that recognise that even private information may legitimately be published when it is in the public interest.

Recommendation:

- The material effect of a successful "right to be forgotten" request should be limited to delisting search results generated on the basis of a search for a person's name.
- The scope of a successful "right to be forgotten" request should be strictly limited to .ru domains.

"Right to be forgotten" procedure

While ARTICLE 19 welcomes some aspects of the "right to be forgotten" procedure, we believe that the Bill fails to provide for sufficient safeguards for the protection of the right to freedom of expression.

- **"Right to be forgotten" request:** ARTICLE 19 welcomes the fact that only private individuals – rather than companies – may claim the 'right to be forgotten'. However, we note that the lack of limitation on reliance by public figures on the "right to be forgotten" means that CEOs of companies may legitimately request the delisting of links to news articles decrying poor management practices or questionable business dealings simply on the ground that

their name is mentioned together with that of the company. In other words, companies are likely to indirectly benefit from the new right. This is especially concerning given the lack of public interest exception and the lack of clarity concerning the types of actions required from search engines in response to a "right to be forgotten" request, i.e. whether the links must be entirely removed or made less accessible when doing a search on the basis of a person's name. We also note that the new right seems to be limited to citizens rather than individuals residing in the territory of the Russian Federation.

We otherwise welcome the requirements that applicants must meet when making a "right to be forgotten" request, including the need to provide the links complained of and the grounds for making the request. The right of search engines to require additional information is also positive, as is the provision of an avenue of appeal before the courts for cases where search engines refuse to comply with a "right to be forgotten" request.

- **Lack of transparency about "right to be forgotten" requests:** ARTICLE 19 is concerned that Article 110 (2)(8) prohibits search engines from disclosing any information pertaining to "right to be forgotten" requests with the exception of unspecified instances prescribed by federal laws. This is problematic in two respects:
  - ***Lack of notification to the linking site***: In practice, the above prohibition means that, pending new legislation in this area, search engines are prevented from notifying linked-to sites whose material may become less or no longer accessible following a successful "right to be forgotten" request. In our view, this constitutes a disproportionate restriction on the right to freedom of expression of linked-to sites and a breach of their rights to a fair trial and to an effective remedy. We believe that linked-to sites should be given an opportunity to challenge "right to be forgotten" requests and be given a right to appeal decisions made by search engines or the courts. At the very least, they should be allowed to intervene in cases being challenged by search engines before the courts. We believe that a right to be notified would be consistent with the requirements of the right to a fair trial and redress the balance in favour of the right to freedom of expression.

  - ***Lack of transparency in the way in which "right to be forgotten" requests are handled***: ARTICLE 19 is further concerned that the Bill does not include any provisions to ensure transparency and accountability regarding the handling of "right to be forgotten" requests and does not specify what information should be made publicly available. In our view, it is vital that search engines publish sufficiently detailed information about the nature, volume and outcome of de-listing requests to ensure accountability regarding the way in which search engines apply the Bill.

Recommendations:

- The Bill should provide a right for linked-to sites to be notified and at the very least give them an opportunity intervene in cases being challenged by search engines before the courts.
- The Bill should require that search engines publish sufficiently detailed information about the nature, volume, and outcome of de-listing requests.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about ARTICLE 19's work in Europe and Central Asia, please contact Katie Morris, Head of Europe and Central Asia, at katie@article19.org.

This analysis was wholly financed by the Swedish International Development Cooperation, Sida. Sida does not necessarily share the opinions herein expressed. ARTICLE 19 bears the sole responsibility for the content of the document.