The Inadequacy of Current Remedies for Violation of Data Subjects' Rights and How to Fix it

Alexander Savelyev

Associate Professor, International Laboratory on Intellectual Property and Information Technology Law, National Research University Higher School of Economics, Candidate of Juridical Sciences; senior attorney, IBM East Europe/Asia Ltd. Address: 20 Myasnitsky Str., Moscow 101000, Russia. E-mail: alexandersavelyev83@gmail.com

Abstract

The paper focuses on civil law remedies for violations of data subjects' rights: claims for damages and claims for compensation of moral harm. Based on an analysis of academic literature, as well as of Russian and international case law, it is argued that, although these remedies are endorsed by the GDPR and other laws, they are inadequate and do not conform to the requirements for an "effective remedy" stipulated by major international legal documents on human rights. The main reasons are: 1) difficulties in proving the fact and the amount of a legally recognized category of damage because the typical consequences of data privacy violations (e.g. the chilling effect caused by dataveillance, negative emotional reactions, etc.) are not considered legally significant by the courts; 2) inability to prove with a substantial degree of certainty a causal link between the violation and the damage incurred because such damage occurs remotely and within complex flows of data. This produces an imbalance in the enforcement of data protection laws so that public law remedies such as administrative fines predominate. This approach is not compatible with the goals of empowering the individual and ensuring control over usage of one's data because there cannot be effective control without an effective remedy to enforce it. In practice this leads to under enforcement of data protection laws because under-resourced data protection authorities cannot address most of the violations that pertain to data protection. A new type of remedy that would resemble the statutory damages applicable to copyright infringement in some jurisdictions should be introduced. Its punitive and decentralized nature would become an additional incentive for data controllers to invest in compliance with data protection laws. From a long-term perspective, it may facilitate including individuals in management of their personal data, without which it would be impossible to effectively address the risks brought about by massive and ubiquitous data processing and algorithmic decision-making.

Keywords

privacy, data protection, compensation, moral harm, effective remedy, statutory damages.

Acknowledgements: This paper was prepared as part of the Basic Research Program at the National Research University Higher School of Economics (HSE) and supported by a subsidy from the "5–100" Russian Academic Excellence Project.

For citation: Savelyev A.I. (2020) The Inadequacy of Current Remedies for Violation of Data Subjects Rights and How to Fix it // *Legal Issues in the Digital Age,* no 2, pp. 24–62.

DOI: 10.17323/2713-2749.2020.2.24.62

Introduction

It is a well-known axiom that a right without remedy is not a right at all. Therefore, any right should be accompanied by a remedy for its breach, and that remedy should be effective — especially so if a fundamental right of a person is at stake[1]. The right to protection of personal data is treated as a fundamental right in the EU[2]. In the Russian Federation, the right to protection of personal data is considered a part of the constitutionally guaranteed right to respect for private and family life[3]. A right of this kind should definitely have adequate remedies for its breach.

Existing international documents impose certain obligations on governments to provide such remedies for breaches of fundamental rights. According to the United Nations, "as part of their duty to protect against business-related human rights abuse, States must take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy." The obligation of states to ensure that any legislative provisions incorporating or implementing fundamental rights are in fact effective is stipulated in other international documents, e.g. in Article 2 of the International Covenant on Civil and Political Rights[4] and Article 13 of the European Convention on Human Rights[5]. EU documents also contain

[1] See Art. 25 of the UN Guiding Principles on Business and Human Rights. New York, 2011, p. 27. Available at: https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf (accessed: 01.08.2020)

[2] Art. 8 of the EU Charter of Fundamental Rights.

[3] Art. 23 and 24 of the Constitution of the Russian Federation; Art. 2 of Federal Law on 27 July 2006 No. 152-FZ "On personal data".

[4] "Each State Party to the present Covenant undertakes: (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; (c) To ensure that the competent authorities shall enforce such remedies when granted."

[5] "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

similar provisions in Article 47 of the Charter of Fundamental Rights of the European Union[6] and Article 19 of the Treaty on European Union[7]. The European Court of Human Rights (ECHR) has interpreted effectiveness to mean that the remedy must be capable of providing redress in respect of the applicant's complaints and that it offers reasonable prospects of success within a reasonable timeframe[8].

Calling for effective remedies for violation of data subjects' rights is not only supported by academic studies but also has definite foundations in the prevailing framework of international law.

Violation of a data subject's rights may incur different types of liability for a data controller. Some of these liabilities fall within public law and have a purely punitive purpose, e.g. administrative and criminal liability. Others like reimbursement of damages or compensation for moral harm are "horizontal" in nature and have a compensatory purpose.

Public law remedies and a punitive tendency in the enforcement of data protection laws are prominent in both Russian and foreign case law. Administrative fines are the main kind of sanctions imposed on data controllers that are liable for breach of personal data regulations and in particular of data subjects' rights[9]. Data subjects may sometimes benefit from administrative fines or the threat to apply them, e.g. through access to their personal data or its deletion; but they do not receive monetary compensation themselves under a system of administrative fines. Administrative fines imposed on a data controller by a court or a data protection authority (DPA) in response to a violation of data subjects' rights are paid to the government rather than to the individual concerned.

However, a breach of data subjects' rights may result in material or non-material damage to natural persons, such as loss of control over their personal

[6] "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."

[7] "Member States shall provide remedies sufficient to ensure effective legal protection in the fields covered by Union law."

[8] *Vuckovic and Others* v *Serbia*, ECHR 25 Mar 2014. References: 17153/11 – Legal Summary, 2014, ECHR 387.

[9] This is evident from the preponderance of news reports on enforcement of data protection that describe cases in which an administrative fine was imposed on a data controller by a data protection authority; also, all the discussions about the effectiveness of sanctions on violation of data protection regulations are reduced mostly to debating what the amount of fines should be and whether they are high enough to induce data controllers to comply with the law. There appear to be no reports of high-profile cases in which data subjects received compensation for damages in amounts as large as the administrative fines imposed on data controllers

data or limitation of their rights, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality for personal data protected by professional secrecy, or other significant economic or social disadvantages to the natural person concerned, as is explicitly recognized in §85 of the Recitals to the GDPR.

Discrimination is one of the most common negative consequences of unlawful processing and one of the main risks in applying algorithmic governance throughout a society. For example, if an employer refuses to shortlist a candidate for interview on the basis of an internet search of posted images that reveal a candidate's ethnicity, it may constitute discrimination based on ethnic origin. However, if an employer refuses to interview based on the candidate's posts in a certain group in Facebook, this would also constitute a form of discrimination that may not be clearly prohibited from a legal perspective but is more frequent in circumstances that now prevail. The loss of a job opportunity in either situation can have a great impact on an individual.

Incorrect profiles based on false, irrelevant or sensitive data may also lead to serious negative consequences for individuals, such as inability to qualify for loans from financial institutions. For example, one data broker (ChoicePoint) incorrectly reported a criminal charge of "intent to sell and manufacture methamphetamines" in the file of a specific person. It resulted in immediate rejection of her job applications. She could not even obtain credit to buy a dishwasher. Once notified of the error, ChoicePoint corrected it, and some other companies to whom ChoicePoint had sold her file corrected their reports promptly; but the individual had to request a correction repeatedly from many others and ended up suing one [Q. Mui Y., 2011][10]. Given the access of multiple data controllers to certain kinds of personal data, this may become a typical scenario rather than an exceptional one.

Identity theft also poses a substantial risk. The few statistics available on identity theft in the EU suggest that almost 2% of the EU population (8,2 million individuals) have been affected by identity theft resulting in an average individual loss of €2,500 s or €20 billion at the EU level. The loss to businesses is estimated to be as high as 0,4% of EU GDP[11]. However, the true magnitude of identity theft remains difficult to quantify inasmuch as there is

[10] Available at: http://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHcWII_print.html. (accessed: 01.08.2020)

[11] CSES. Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft: Final Report, 11 December 2012.

no commonly accepted definition for identity theft, it is not often reported to police, and victims are in many cases unaware that they have been targets of identity fraud.

If we acknowledge that personal data breach is a violation of a fundamental right of individuals, then we should agree that the losses which individuals sustain from these data incidents should be properly compensated to them. This idea is reflected in much current legislation. According to Article 79(1) of the GDPR, "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation". Paragraph 146 of the Recitals to the GDPR reinforces the point:

> The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation…. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Data subjects should receive full and effective compensation for the damage they have suffered.

Article 78 in Chapter VIII of the GDPR emphasizes the point that an effective legal remedy is not automatically present whenever remedies are available under national law. For example, the option to lodge a complaint with a supervisory authority according to Article 77 of the GDPR is explicitly mentioned as not constituting an effective judicial remedy inasmuch as supervisory authorities are not considered courts but administrative bodies (albeit vested with special independence) [Kuner C., Bygrave L., 2020: 1135]. In *Schrems* v *Data Protection Commissioner*, the European Court of Justice found that the complete absence of "any possibility for an individual to pursue legal remedies…does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[12]. The GDPR explicitly states that exclusively administrative remedies are insufficient to meet the threshold for an effective remedy.

At the time of writing there are no reports of high-profile cases resulting in compensation to an individual for damages caused by processing of their

[12] *Schrems* v *Data Protection Commissioner*, ECJ, C-*362*/14, 06 October 2015, § 95.

data in violation of GDPR provisions[13]. By contrast, there are a great many instances in which data protection officers levied administrative fines on data controllers[14].

Unlike the GDPR, Article 1(2) of the Russian law on personal data[15] explicitly recognizes two types of private law remedies available to data subjects: the right to claim damages and the right to claim compensation for moral harm. In theory, these types of remedies are intended to address different types of losses. A loss suffered by the data subject may be either economic or non-economic in nature. The type of loss incurred determines the type of remedy to be applied: damages claimed on grounds of an economic loss; and compensation for moral harm claimed on grounds of a non-economic loss. An economic loss is incurred if the interests harmed have a market value which can be assessed according to the economic rules prevailing in that market. Damage which is not economic in nature (such as mental suffering) can only be given a monetary equivalent through the judicial decision to compensate for moral harm. In practice, however, the first remedy (a claim for damages) is not used, while the second one (compensation for moral harm) is not effective enough and does not have much impact in protecting data subjects' rights.

---

[13] There were some cases of the kind when 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 was in force. But they were few in number and attracted very little attention compared to the enforcement of data processing agreements and associated fines for their violation.

[14] Among the most recent reports are an ICO Statement "Intention to fine Marriott International, Inc. more than £99 million under GDPR for data breach", 9 July 2019. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/?fbclid=IwAR1TkwUg_CLdroHQTDVLOmmezfcfTRFiPo-jvPJBgRATT2ANwSkCRVrRP9A) (accessed: 01.08.2020); and "British Airways faces record £183m fine for data breach" reported by BBC News, 8 July 2019 (available at: https://www.bbc.com/news/business-48905907?fbclid=IwAR3ILh0ntXc6usYUgaqWJN4pv3L1BFr5VfSN6eps_SE8tLIyKwn9rzQluyQ (accessed: 01.08.2020); "The Romanian National Supervisory Authority for Personal Data Processing imposes the first fine under GDPR on Unicredit Bank in the amount of 130 000 Euro", 27 June 2019 (available at: https://www.dataprotection.ro/index.jsp?page=Comunicat_Amenda_Unicredit&lang=en&fbclid=IwAR2yvwm5eqWp1Ek2MlrM8XIZPia0AGWhvh9TN7Qoh9DK3H5RTWe3mnru-NE (accessed: 01.08.2020); and also "French DPO (CNIL) imposes fine in the amount of 20 000 Euro on UNIONTRAD", 18 June 2019 (available at: https://www.cnil.fr/fr/uniontrad-company-20-000-euros-damende-pour-videosurveillance-excessive-des-salaries?fbclid=IwAR0I_4gtBwwJ9ZZ_Avm8NLfB3r_cWpXwPST4oB6jXu2bTrEqfx39LJj-WKLQ (accessed: 01.08.2020).

[15] Federal Law "On personal data" No. 152–FZ of 27 June 2006 (with subsequent revisions and amendments). This law is based on international and EU data protection law and was adopted as a part of the implementation measures of Council of Europe Convention No. 108, which has been ratified by Russia.

This paper argues that the problem with ensuring effective remedy arises not only from certain distinctive features in the Russian legal system and its case law, but also from the incompatibility of these remedies with particular aspects of data protection. That incompatibility renders them inadequate for effective protection of data subjects' rights. The best way to flesh out this argument is to proceed with a description of general rules applicable to these remedies followed by an account of public law liabilities for violating a data subject's rights. In the following sections Russian law on these matters is described in detail and also compared to EU and international law.

1. Overview of private law remedies available to data subjects

1.1. Damage claims for breaches of data subjects' rights

A claim for damages is one of the most common "horizontal" remedies available for breach of one's civil rights. A damage claim addressed by a data subject against a data controller is contestable. By default, such a claim will refer to a tort because the obligations of a data controller are established directly by law and do not require any agreement concluded with the data subject.

However, it may be argued that a claim for damages may in certain limited circumstances be contractual in nature because specific obligations of the data controller concerning processing personal data have been explicitly stated as a part of the contractual terms that were accepted by the data subject. For example, it may be the case that a data subject has expressed consent by means of a clickwrap agreement (e.g. to the terms of use or privacy policy presented in an online interface) that covers processing of personal data in the course of providing services. The fact that these terms constitute a part of the online contract, which the data subject accepts in a way similar to accepting the other terms of the contract, supports the argument that breach of these contractual provisions concerning personal data processing should be treated the same as a breach of the other provisions of the contract.

In the event that there are no contractual relations between the data controller and the data subject such that the conditions applicable to processing personal data are stated as a distinct set of terms consented to by the data subject, any claim for damages will definitely be based upon a tort.

Regardless of the nature of the damage claim raised by the data subject (a topic which deserves more extensive study), there are no substantial differences in the burden of proof placed on the data subject. In either case that burden is very difficult to manage.

None of these claims (whether contractual and non-contractual) are mutually exclusive. Data subjects may choose the basis of their claims at their own discretion.

Regardless of the nature of the relations forming the basis for the claim, the burden of proof imposed on data subject will consist of the following items:

fact of violation of the data subject's right which has been granted by the law;

amount of loss incurred;

causal link between the violation and the amount of loss claimed.

The data controller's fault is not a part of the burden of proof because contract law presumes that the data controller acting as a commercial entity is at fault whenever a data subject makes a claim a data controller. However, a determination of fault may have an impact on success of the claim, and that will also be covered in the discussion that follows. Let us take a closer look at those elements in the burden of proof and outline the main difficulties facing data subjects in pursuing their claims.

1.1.1. The fact of violation of the data subject's right which has been granted by the law

Violation of a data subject's right should be proved by presenting evidence that the data controller failed to comply with specific provisions of the data protection regulations as they pertain to the data subject. The most typical types of violations of a data subject's rights are:

unlawful transfer of personal data from data controllers (employers, public authorities, mobile operators, credit institutions, etc.) to third parties;

improper and excessive collection and storage of personal data by public authorities, or by commercial entities (telecom operators, supermarket chains, banks, etc.) without legitimate purpose, proportionality and sufficient guarantees of security;

storage of inaccurate information;

manipulation of inaccurate personal data stored and processed legally, including by means of algorithmic decision-making;

publication of personal data in the media or on the internet;

denial of access to personal data held by the data controller or insufficient responses to requests for access to personal data;

refusals to correct, delete and block information in personal data files or insufficient responses to requests for corrections, deletion and blocking of information in personal data files[16].

In some cases when these violations are encountered in the course of interacting with a data controller, it is not very difficult to prove the fact, e.g. when there is denial of access to information about personal data processed or failure to delete personal data upon request. A copy of the communications between the data subject and data controller may suffice for the purpose. Certain other violations, such as data leakage, may sometimes be established by referring to information which appears in mass media. Other violations, such as unlawful disclosure of personal data to a third party, may become apparent during contact with other persons when they refer to information that was disclosed only to the data controller (direct marketing, etc.), although inferences of this kind can also be very difficult to validate.

Of course, not all of the many violations of data protection laws committed daily by data controllers will be visible to data subjects. Those violations may be come to light only after a detailed audit of a particular data controller by a data processing authority (DPA) or as a result of whistleblowing. But the mere fact that there are some violations which cannot be discovered by the data subject does not mean that there is no need to have legal instruments empowering them in other situations. As has aptly been said, "Nobody made a greater mistake than he who did nothing because he could do only little"[17].

1.1.2. Amount of loss incurred

The second element that the plaintiff has to prove in order to succeed with a damage claim is the fact of losses and their amount. Financial loss is rarely encountered in data privacy violations[18]. It typically comes up in identity theft cases that involve unauthorized money transfers or lost opportunities to qualify for a loan. In these exceptional cases proving the

[16] For a more extensive listing of kinds of violations, see, e.g.: Access to data protection remedies in EU Member States published by the EU Agency for Fundamental Rights (FRA), p. 26.

[17] This is usually attributed to Edmund Burke.

[18] According to the EU FRA, few complainants in most of the sixteen EU member states have suffered financial losses as a result of data protection violations. EU FRA, Access to data protection remedies, p. 28.

amount of damages should not be much of a problem. But it will be difficult in most other cases for an individual to calculate the amount of damages caused by violation of their rights as a data subject because of the intangible and non-pecuniary nature of the harm. In most cases those calculations will be speculative and fall short of being persuasive in court.

Recent amendments to the Civil Code of the Russian Federation have established a more liberal approach since 2014 to proving the amount of damages claimed. Those amendments have made proof to a reasonable degree of trustworthiness allowable (Article 393 (5). In contrast to earlier case law, the courts cannot now dismiss a damage claim in its entirety on the sole grounds that its amount was not proven with sufficient precision by the plaintiff. This view is now a feature of Russian case law. According to the Supreme Court of the Russian Federation, failure to prove the exact amount of damages incurred does not relieve the party that committed a breach from liability. In such cases the court should determine the amount of damages for which compensation is due[19]. These clarifications and legislative developments have made things easier for plaintiffs, but they do not release them from the requirement to provide objective evidence for financial loss in general.

For damage claims based on contractual relations between a data controller and a data subject, specific contractual provisions relating to exemptions and limitation of the data controller's liability may apply. While those provisions may be enforceable generally based on the principle of freedom of contract, some of them may be invalidated as unfair contract terms in accordance with applicable legislation[20], or they may be rendered void on grounds of violating mandatory provisions of the data protection regulations. Resorting to those avenues for claiming damages imposes an additional burden on data subjects because of the effort and expense involved in suits of that kind.

1.1.3. Causal link

Finally, the data subject has to prove that there is sufficient causal linkage between the data controller's act and the loss suffered. In most cases

[19] Section 9 of the Review of Case Law of the Supreme Court of the Russian Federation, No. 2, 2016.

[20] See, e.g.: Unfair Contract Terms Directive 1993; Art. 428 of the Civil Code of the Russian Federation.

this is almost impossible to prove due to the extremely complex nature of information flows. As noted authority on privacy issues Daniel Solove puts it: "There are too many entities collecting and using personal data to make it feasible for people to manage their privacy separately with each entity. Moreover, many privacy harms are the result of an aggregation of pieces of data over a period of time by different entities." [Solove D. 2013: 1881]. The remote nature of the link between data protection violations and harms incurred is recognized by other legal scholars as well [Lynskey O., 2015: 209]. A speaker at an OECD roundtable used the metaphor of a blank cheque to describe the situation and argued that, when someone reveals private data to others, they are signing a blank cheque that "may never come back to her, or may come back to him, or may come back for an indeterminably small or large price to pay. That price could be mild embarrassment, an annoying spam, or a devastating case of identity theft." [Acquisti A., 2010: 26]. The Electronic Privacy Information Center (EPIC) argues that "opaque industry practices result in consumers remaining largely unaware of the monitoring of their online behavior"[21].

Hence, it is not possible for a data subject with limited knowledge and limited understanding of personal data flows to single out a clearly defined cause and effect relation from an entire chain of information flows and determine the potential seriousness of the harm. There are too many factors affecting the overall harmful result, and therefore it is not possible to isolate a particular unlawful act of the data controller from the overall picture and then show a causal link as a "mechanistic" pattern.

Disputes arising from information processing are substantially different from conventional commercial disputes where it is far easier to show a causal link (e.g. a vendor fails to deliver goods and that results in penalties imposed on the buyer by his counterparty for failure to deliver a product in which the missing goods were an important element). For information flows the damage is too remote and consequently may not be legally relevant in terms of liability. For example, a data controller may find it useful to create a centralized database containing various types of personal data, but the database may have a single point of vulnerability to large-scale identity theft. Individual data subjects could object to keeping certain kinds of information in the database on the grounds of that the data minimization prin-

[21] EPIC, Search Engine Privacy. Available at: https://epic.org/privacy/search-engine/ (accessed: 14.07.2020)

ciple requires that only relevant and necessary personal data be retained (although the data controller could counter that objection by claiming that keeping the data results in greater efficiency and is of legitimate interest). Consider the following scenario: certain pieces of personal data, which were not strictly necessary for the data controller's operations but were included in the database, might subsequently fall into the hands of a third party who in turn processes it further and forwards the results to another person; that person might have their data hacked and then used for fraudulent transactions. It would be impossible to the individual to link the fraud to the initial breach of the data minimization principle by the initial data controller.

The difficulty data subjects face in proving causation is acknowledged by legal specialists. For example, in her analysis of the GDPR, Emmanuela Truli argues that "the person who has suffered damage may not easily have had access to information proving that e.g. he did not get a job offer or credit due to the incorrect information collected, stored or disseminated by the controller, or the damage may not have been immediate." [Truli E. et al, 2017: 312]. Other academic specialists in law and technology observer observe that "because of information asymmetries, data subjects are often unaware (or at least less conscious than data controllers and other entities) about the nature, extent and use of collected data." [Lazaro C., Le Métayer D., 2015: 10]. To sum up, it is arguable that the causal link is the most difficult part of the burden of proof imposed on data subjects in pursing their claims for damages.

1.1.4. Fault of the data controller

There is a presumption in Russian law that the data controller is at fault in damage claims on both contractual and tort grounds. The GDPR adopts a similar approach, when describes the conditions under which controller or processor won't be held liable: "A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage"[22]. Strictly speaking, the fault of the data controller is not a part of the overall burden of proof imposed on a data subject by Russian law. However, it deserves some attention because the data controller's fault may affect the success of a data subject's claim for damages.

[22] Art. 82(3).

A data controller's fault may be based upon intent or negligence[23]. Many types of personal data breach may be attributable to intent, which is often influenced by the substantial economic benefits that the data controller may gain from the unlawful use of personal data. A hospital might provide patients' information to other companies in its group or to third party companies for use in direct marketing; or a provider of cloud services may secretly comb through documents stored by data subjects for the same reasons [Truli E., 2017: 317]. Other types of violations of data protection laws, such as failure to implement adequate technical measures to protect personal data, may be attributable to negligence. But in practice this distinction between intent and negligence does not play a substantial role in assessing the merits of the claim: any fault will suffice.

Strict liability may apply under some conditions. This is the case when the liability is connected with the commercial activity of the defendant and has a contractual nature. If a data controller breaches terms concerning data processing expressed in a contract with data subjects and the contract was concluded as part of the commercial activities of the data controller, then the controller will be liable regardless of the absence of fault (Article 401(3) of the Civil Code of the Russian Federation). The data controller may be exempt from liability only if they prove that the violation was due to force majeure. Actions of third parties, especially when they are potentially foreseeable, such as hacker intrusions, cannot be treated as force majeure[24]. Thus specifying relations between the data subject and data controller in an agreement covering personal data processing in a contractual format can be advantageous for the data subject because it can support a stricter treatment of fault; however this advantage may be diminished if the contract contains clauses that limit liability and exclude warranties.

[23] According to Art. 401(1) of the Civil Code of the Russian Federation, "a person is recognized as not at fault, if with the degree of care and caution that was required of him by the nature of the obligation and the conditions of commerce, he has taken all measures for the proper performance of the obligation". The form of fault (intent or negligence) is irrelevant to the amount of damages claimed; any form of fault for a data controller is a sufficient basis for claiming damages.

[24] However, not all courts would share this view. For example, in one of the disputes considered by a Korean court an overseas hacker took personal details relating to 18 million customers of Auction, of whom 145,000 (organized in ten groups) brought "collective" individual suits. In 2010 the Seoul Central District Court held in favor of Auction (upheld on appeal by the Seoul High Court in 2013), finding that its security was not at fault (Auction argued that it was not mandatory to install firewalls at that time because they were not very effective) and apparently also because of the swift response by Auction's management. This is described in: [Greenleaf G., 2014: 132].

1.1.5. Difficulties in legal representation of claims

The complexity of the facts which must be considered in disputes concerning damage claims for violation of a data subject's rights may make legal representation quite expensive, and the time required for litigation and its other general costs may be also be prohibitive for data subjects. By contrast, data controllers, especially the larger companies, have almost unlimited budgets for litigation and are further motivated to litigate in order to prevent the establishment of unfavorable precedents in case law. When the data subject's claim is unlikely to prevail or the amount of damages awarded would probably be small, lawyers have little incentive to take on lawsuits for data subjects. Data subjects for their part are mostly unwilling to pay high legal fees for disputes of this kind, especially when there is little chance of success. The end result is that data subjects in private law disputes with data controllers usually cannot secure legal representation.

Singapore provides the best practical illustration of these points. According to Graham Greenleaf's survey of Asian privacy law, "given the costs of initiating litigation in Singapore, and the risks of costs being awarded against the plaintiff, there is therefore no low-cost or low-risk means by which Singaporean data subjects can seek modest amounts of compensation for data protection breaches."[Greenleaf G., 2014: 313].

1.1.6. Overview of the current situation

In many jurisdictions the prospects for civil law remedies available to data subjects are not very encouraging. As Greenleaf finds, although Hong Kong has a relatively litigious culture in which there are frequent defamation suits, compensation claims there show that the "system did not work". It is believed that only one claim of this kind during the first fifteen years since new regulations on data protection (Personal Data Ordinance of 1995) were adopted has been successful, and there was other one misconceived attempt [Greenleaf G., 2014: 115]. There have been no cases of compensation or damage claims by data subjects in India, nor are any reported in Macao, although its data protection law has been in force since 2005 and is considered one of the strongest (at least on paper) [Greenleaf G., 2014: 268, 283, 519][25]. In

[25] The only evident exception among Asian data privacy laws is in South Korea where some suits brought by data subjects have been successful.

Germany as well non-contractual claims by data subjects based on breaches of data protection rules are viewed as exceptional [Truli E., 2017: 318]. According to the EU Agency for Fundamental Rights (FRA), civil claims are rare because complainants in the sixteen EU member states surveyed were reluctant to initiate court proceedings because of high costs, lengthy procedures and a perceived need to be represented or assisted by a lawyer[26].

In sum, damage claims by data subjects against data controllers are rarely made because they fail to take into account the actual nature of the factors involved in data protection; therefore resorting to such claims cannot be considered effective as a protection for data subjects' rights. According to the report prepared by the European Union Agency for Fundamental Rights, which is one of the most comprehensive studies of the enforcement of data protection remedies, "the available remedies in this sphere are not effective enough"[27]. Let's now turn to the second type of remedy available to the data subject — compensation for moral harm.

1.2. Compensation for moral harm from breaches of data subjects' rights

1.2.1. General criteria for compensation

The underlying requisites for recovery of non-material damage in various countries vary greatly, although there are generally two basic models. Some European legal systems regard every kind of damage as in principle recoverable. The remainder adopts a contrasting approach in which non-material damage is generally compensable only when the law explicitly deems it so.

The Russian law "On personal data" follows the second approach and explicitly provides for compensation of moral harm for violation of data subjects' rights. Data subjects will have to prove the same things required for damage claims: the fact of violation of the data subject's rights granted by the law; the fact of harm; and the causal link between the violation and the moral harm. The main difference from the requirements for claims of dam-

[26] EU FRA, Access to data protection remedies, p. 35.

[27] Comment on the EU FRA report, Access to data protection remedies in the EU Member States, posted 7 February 2014 on the website of the Human Rights House Foundation. Available at: https://humanrightshouse.org/articles/fra-report-access-to-data-protection-remedies-in-eu-member-states/ (accessed: 01.08.2020)

ages is in the second requirement: the nature of a moral harm claim precludes requiring the plaintiff to produce detailed calculations of its amount.

Because this kind of remedy is intended to compensate for non-pecuniary losses, it seems at first glance as if it may be a more suitable remedy for violations of data subjects' rights. According to the clarifications of the Supreme Court of the Russian Federation, moral harm may occur in the form of mental suffering caused by estrangement from relatives, the impossibility of continuing active social life, loss of employment, disclosure of family or medical secrets, physical pain, etc.[28]

In contrast to Russian law, European law considers potential types of non-pecuniary loss more broadly and includes "impairment of the quality of life" in addition to pain and suffering (VI.–2:101 (4) (b) of the EU Draft Common Frame of Reference). Commentary on the Draft Common Frame of Reference (DCFR) explains: "typical examples are provided by infringements of incorporeal rights of personality (among others, incursions into spheres of privacy; derogatory statements which have as a consequence a negative impact on the social profile of the person concerned)." [Von Bar Ch., Clive E. et al., 2009: 3040]. While the concept of non-pecuniary loss as "impairment of the quality of life" may adequately reflect the consequences of some violations of data subjects' rights, a narrowly literal interpretation may not address many types of harm related to privacy.

1.2.2. Russian approach

From a technical standpoint, the list of grounds provided by the Supreme Court of the Russian Federation for claiming moral harm from mental suffering is not exhaustive and may extend to most of the possible grounds for claiming privacy-related mental suffering: damage to reputation, discrimination, interference of third parties in private matters, etc. However, actual case law diverges sharply from this broad approach.

The mere statement by the data subject that a certain violation of their rights caused distress and emotional suffering is routinely rejected by Russian courts. As one of the courts put it, "the mere fact of violation of data subjects' rights does not provide a basis for claims for damages or compensation of moral harm"[29]. According to the established case law, the pres-

[28] Art. 2 of Decree of Plenum of the Supreme Court of the Russian Federation "Some issues in the application of legislation on compensation for moral harm". 20 December 1994. No. 10.

[29] Appellate judgment of the Novosibirsk Region Court. 31 July 2017. No. 33-10465/2017.

ence of moral harm is to be confirmed by verifiable evidence, e.g. a record obtained from a medical institution of a pertinent diagnosis (depression or a nervous disorder)[30]. It is evident that in most cases a data subject will not be able to present such "bullet-proof" evidence.

It may come as a surprise that this position of the Russian courts is on the same page with the DCFR when it states that "negative emotional responses such as annoyance, anger, disgust and repulsion which lie within the spectrum of normal, everyday feelings *are not enough to meet the threshold of physical or mental suffering necessary to succeed with the claim*" (italics added.- A. S.) [Von Bar Ch., Clive E. et al., 2009: 3040]. However, these emotions are the most typical ones when particular rights of data subjects' are violated. Failure to recognize the legal significance of such violations deprives data subjects of an effective remedy for protecting their rights and *de facto* relieves the data controller from liability and responsibility toward the data subject for such violations. This is especially concerning if we examine the position of the European Court of Justice (ECJ), which held that even certain types of fear may have legal significance. In its landmark decision invalidating the EU's Data Retention Directive[31], the ECJ maintained that the mere fact of performing certain kinds of processing, such as profiling or data retention, is '"likely to generate in minds of persons concerned the feeling that their private lives are the subject of constant surveillance"[32].

In addition to the way current legal remedies fail to recognize the distinctive features of privacy-related harm, there is also a problem with arriving at the amount of compensation for moral harm. According to Russian law, the courts have a substantial degree of discretion in determining the amount of monetary compensation awarded when hearing a claim for compensation of moral harm. The court is to set it:

> depending on the nature of the physical and moral suffering caused to the victim and also the degree of fault of those who caused the harm in in the event that the fault is a basis for compensation for harm. In de-

[30] See e.g. Appellate judgment of the Court of Moscow City. 22 December 2015. No 33-48112/2015.

[31] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105)

[32] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v. Ministry of Communications, Marine and Natural Resources and Others and Kärntner Landesregierung und Others, 2014, OJ C175/6, § 34.

termining the measure of compensation for harm, the requirements of reasonableness and justice must be considered. The nature of physical and moral suffering shall be evaluated by a court taking into account the factual circumstances under which moral harm was caused and the individual peculiarities of the victim[33].

The GDPR has established a more detailed list of factors which the courts should take into consideration when setting the amount of compensation:

the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor[34].

Although in theory judicial discretion in setting of the amount of compensation should simplify things for data subjects by removing the need to prove the precise amount of loss suffered, in practice the courts do not exercise this discretion much to the advantage of data subjects.

Russian case law shows how this judicial discretion plays out in fact. The average amount of compensation for moral harm that is awarded to data subjects in Russia varies from 500 to 10,000 rubles (that is approximately from €7 to €130). For example, compensation in the amount of 500 rubles was awarded to a data subject for having information about their failure to make timely public utilities payments posted by a data controller in the public hall of the subject's apartment house[35]. The same amount of compensation was awarded for sending unsolicited SMS marketing messages[36]. The sum of 10,000 rubles was awarded for using an individual's personal identification in an example of how to fill in an application form with the Pension Fund because the personal data had been made publicly available without consent of the data subject[37]. In another case 10,000 rubles were awarded for processing the personal data of an individual to draft a loan

[33] Art. 1101(2) of the Civil Code of the Russian Federation.

[34] §146 of the Recitals to the GDPR.

[35] Cassation judgment of the Saratov Regional Court. 14 February 2012. No. 33-489.

[36] Appellate judgment of the Novosibirsk Regional Court. 31 July 2018. No. 33-7489/2018.

[37] Judgement of Primorsky District Court. 14 July 2014. No. 33-5960.

agreement, which was then used to make legal claims against the individual even though the agreement was not valid because the signature was forged[38].

Many judgments of Russian courts on compensation of moral harm for violation of data subjects rights' are issued without an indication of the amount awarded, which is in keeping with the regulation on maintaining anonymity in the decisions of the courts. But there is no reason to believe that such "anonymized" judgments contain awards substantially different from the ones described above. Cases with much higher awards would be noteworthy enough to be disclosed in other ways, e.g. in mass media and through social networks. Even in those rare cases where the court of first instance has awarded compensation in amounts exceeding the averages indicated above, an appellate court has frequently reduced them[39].

There are two reasons for the negligible amounts of compensation for moral harm in Russia. First, there are no established methods for calculating compensation for moral harm, nor are there any guidelines for their calculation that are more detailed than the provisions of the Civil Code described above [Erdelevskiy A., 1999: 192]; [Marchenko S.V. et al., 2004]. In these circumstances, courts do not provide any explanation of how they arrived at the specific amount of money awarded, and they are reluctant to make themselves conspicuous by departing from the usual small amounts in earlier case law. The courts seem to have become captives of the previous case law and cannot change their approach without legislative intervention. The second reason is that Russian courts tend to acknowledge the occurrence of moral harm more readily when it also affects the material well-being of a person. For example, when harm to the health of a person seriously affects their ability to work and causes an obvious decline in their standard of living, the courts are much more likely to allow compensation for moral harm in addition. Here again we see a misunderstanding of the nature of the privacy harm and of the way data privacy violations produce distress.

The nominal amount of compensations for moral harm awarded by Russian courts has come under heavy criticism in Russian legal discourse [Bogdanova O.V., 2017]; [Tabunschikov A.T., 2017] and even by Russian government authorities. Specifically, in its annual report for 2017 the Russian Service for the Protection of Consumers (Rospotrebnadzor) indicated that the compensation for moral harm when consumer rights are violated

[38] Appellate judgment of the Saint Petersburg Court. 16 August 2018. No. 2-293/2018.

[39] Appellate judgment of the Saint Petersburg Court. 16 August 2018. No. 2-652/2018 (in this case the appellate court decreased the amount of compensation from 30,000 rubles to 10,000 rubles).

should not be 5,000 or 10,000 or even 25,000 rubles, but much higher[40]. Rospotrebnadzor also argues for a uniform way to calculate moral harm[41]. While these recommendations may improve the case law in consumer protection, they are unlikely to be applied to compensation for moral harm resulting from violation of data subjects' rights. Piecemeal solution here will not be enough; more fundamental changes are needed.

1.2.3. European approach

European case law is becoming more generous with the amounts of compensations awarded, but still leaves much to be desired. According to a European Union Agency for Fundamental Rights Report:

> the amounts awarded vary greatly between Member States. Austria for instance, sets an upper limit of €20,000 for non-pecuniary damages, but the range of cases in other Member States suggests that awards of compensation are often much lower, ranging from €300 to €800 in Finland, up to €600 in Sweden, and from €1,200 to €12,000 in Poland[42].

Case law in the UK deserves a closer look, as some of the arguments put forth there and the way they were countered have substantial weight outside of the UK's jurisdiction and may help to illustrate better the main ideas of this paper.

Until recently UK case law could not boast of compensation for moral damage from privacy-related misdeeds. One of the landmark cases is *Google Inc.* v *Vidal-Hall and others*[43]. This is the first case, where the Court of Appeal of England and Wales recognized moral damages under the UK Data Protection Act of 1998. Prior to that case, compensation for distress which was not accompanied by pecuniary loss had not been awarded by UK courts[44].

[40] Protection of Consumers in the Russian Federation in 2017 A Government Report. Moscow, 2017, p. 150 (in Russian)

[41] Idem.

[42] EU FRA, Access to data protection remedies, p. 21.

[43] Google Inc v Vidal-Hall [2015] EWCA Civ 311.

[44] Section 13 (2) of the UK Data Protection Act 1998 provided that "an individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes." A literal interpretation of this provision leads to conclusion that, absent certain pecuniary loss or processing for special purposes (journalistic, literary or artistic), no compensation for distress is possible. This approach was supported by Buxton LJ in Johnson v Medical Defence Union, 2007, EWCA Civ 262.

Moreover, one of the grounds on which it was argued that the UK had not implemented the Data Protection Directive correctly was that the "UK Act does not provide for 'moral damages'"[45].

The Court of Appeal was asked to examine the claim in this case that the defendant had misused private information, acted in breach of confidence, and in breach of its statutory duties under the UK Data Protection Act by tracking and collating information relating to the claimants' internet usage on the Apple Safari browser without their knowledge and consent. That information was subsequently used for Google's targeted advertisements. It was alleged that their personal information was not respected despite the fact that the claimants had set their privacy settings in the browser to block third party cookies[46]. The Court of Appeal, satisfying the claim for misuse of private information, highlighted the status of data protection as a fundamental right in the EU Charter of Fundamental Rights, suggesting that it would be odd if this right could be violated with "relative impunity by a data controller, save in those rare cases where the data subject had suffered pecuniary loss as a result of a breach"[47]. The conclusion was that compensation can be awarded even though no actual financial loss occurred and that any other approach is not compatible with the concept of "effective remedy" under Article 47 of the EU Charter of Fundamental Rights[48].

While no specific reference is made to moral damage or moral harm in the GDPR, it does state in Article 82(1) that "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." The provisions of Article 82 provide a comprehensive framework for such claims, which can be used to minimize the discrepancies between the rules for liability that were put in place by various national laws under the EU's Data Protection Directive of 1995.

Apart from that clear indication that both pecuniary and moral types of damages may be compensated, the GDPR also states that they may be claimed against data processors that have not complied with the GDPR ob-

[45] Google Inc v Vidal-Hall, §70.

[46] Similar cases have been brought against Google in the United States, leading to a US$22.5 million Federal Trade Commission fine and a US$17 million settlement with state attorneys general. Available at: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; https://www.insideprivacy.com/united-states/google-settles-safari-tracking-charges-brought-by-state-ags-for-17-million/ (accessed: 01.08.2020)

[47] Google Inc v Vidal-Hall, §78.

[48] Google Inc v Vidal-Hall, §91.

ligations specifically directed to processors or where they have acted outside or contrary to lawful instructions of a data controller. Therefore, the distinction between data controllers and data processors is somewhat irrelevant in adjudicating compensation claims.

In general, the wording of Article 82 of the GDPR supports the conclusion that compliance with the GDPR requires a two-tier enforcement system consisting of "a mutually reinforcing combination of public and private enforcement that blends public fines with private damages." [O'Dell E., 2017: 3][49]. The reality is that almost all enforcement is carried out through the public enforcement tier due to the ineffectiveness of the private one.

1.2.4. US approach

US law contrasts with the EU and Russian approaches by retaining a narrow definition of privacy harm. It focuses on pecuniary losses and does not allow compensation for moral damage from privacy-related malfeasance. For example, in *Smith* v *Chase Manhattan Bank* the defendant sold its customer information to third parties in violation of its privacy policy and earned a commission on targeted sales by those third parties to the plaintiff and others. The plaintiffs' contractual legal claim was rejected by the court on the grounds that they could not prove any actual harm inasmuch as they were "merely offered products and services, which they were free to decline"[50].

It was also argued that potential claims based on the fear that surveillance deters individuals from exercising their right to freedom of expression guaranteed by the First Amendment to the US Constitution or that the information may be misused in the future are likely to fail due to Supreme Court's rejection of such a "chilling effect" in its *Laird* v *Tatum* decision. In that case the Supreme Court found the claim without merit, as it did not show any objective harm or threat of future specific harm[51]. Claims against government agencies for damages from invasion of privacy based on the Privacy Act 1974 must also demonstrate "actual damages", and the Supreme Court has held that distress is insufficient to amount to "actual damages" for these purposes[52].

[49] Available at: https://ssrn.com/abstract=2992351 (accessed: 01.08.2020)

[50] Smith v Chase Manhattan Bank 741 NYS2d 100.

[51] Laird v Tatum 408 US 1 (1972).

[52] Doe v Chao 540 US 614 (2004); Federal Aviation Administration v Cooper 566 US 284 (2012).

These examples show that many courts prefer a conservative approach in cases where no specific moral harm has been proven and either dismiss the case entirely or award compensation in amounts so minimal that data subjects are discouraged from vigorously defending their privacy rights. There are exceptions of course, but they do not change the restrictive *status quo*.

2. Some Consequences of Current Approaches

The weak enforcement of individuals' claims for damages and compensation for moral harm justifies a number of concerns.

2.1. Data protection legislation may become a tool primarily for facilitating the state's own agenda

The preponderance of administrative fines among the liabilities attached to privacy-related harms skews the balance away from private law remedies, in which the data subject is the "master" of their claim and the beneficiary of its successful outcome, and toward public law remedies, in which a state authority advances the claim and derives all the financial benefit from its success. That imbalance conflicts with the ideas that individuals should be empowered by giving them free choices and that "natural persons should have control of their own personal data"[53].

Those ideas are derived from a conception of privacy that includes control over information[54]. According to Alan Westin, author of Privacy and Freedom privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [Westin A., 1967: 7]. According to philosopher Charles Fried, "privacy is not simply an absence of information about us in the minds of others, rather it is the control we have over information about ourselves." [Fried C., 1984: 209]. In other words, the rights of data subjects are not negative rights understood in a passive or nega-

[53] Recital 7 to the EU GDPR. One of the aims of the new regulation outlined in EU policy documents was to "put individuals in control of their own data". See: European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 Final, p. 2.

[54] As a rule, violation of the right to data protection leads to a violation of the right to privacy, at least in its informational aspect, but a privacy violation does not necessarily result in a violation of the right to data protection.

tive sense as the right to be left alone, but instead they are *proactive* rights which facilitate active involvement of individuals in managing their data. Individuals should therefore be instrumental in making data protection law more effective.

However, there cannot be control without the opportunity to mount an effective defense of a right, including the possibility of defending it at the discretion of its owner. Where there is no effective access to justice in order to obtain redress, there is no additional accountability for those processing data; hence, there is no true control. Outsourcing enforcement solely to data processing authorities creates merely an illusion of control by data subjects because the DPA is a state authority performing its functions primarily in the interests of the state rather than in the interests of the data subject. One's privacy will be valued less than matters of national sovereignty over information or efficiency in the operations of the state authority.

Personal data regulations have already become "dual use" in nature and pursue two different purposes. One officially declared purpose is to respond to the need for protecting the interests of data subjects. A second more covert purpose is to implement a political agenda of increasing control over the internet. A vivid example of this approach is data localization regulations, which have the officially proclaimed purpose of protecting individuals from misuse of their information, but in fact are intended to facilitate law enforcement, increase growth in the local data center market, and provide conditions suitable for keeping the nation's internet autonomous and under national control.

Russia is no newcomer to using personal data legislation for such political purposes. In his comprehensive examination of cross-border data flows and the attempts to control them, Christopher Kuner finds that national regulation of data protection (and of transborder personal data flow in particular) is frequently a way to protect national interests and national sovereignty. Although the examples provided by Kuner date from the 1970s and '80s, they still seem quite relevant to current concerns [Kuner C., 2013: 30].

There are other items in a state agenda for which "assistance" from a DPA may come in handy, such as protecting local companies or advancing economic and geopolitical ambitions. If you ask any major internet company why it made a certain decision that has an impact on processing personal data, you will hear some variation of "to improve the user experience". But as Frank Pasquale, a persistent critic of the way privacy is succumbing to business interests has pointed out, "we all know that it's only a certain kind

of user experience that is really valued and promoted…. the more a person clicks on ads and buys products, the better …. the more a person draws other potential ad clickers in — the more valuable they become." [Pasquale F., 2015: 166]. Such an approach certainly results in processing more and more information from individuals and sharing it with more parties. Because it may facilitate the growth of data-dependent companies and of certain associated segments of the national economy, a DPA may give a sympathetic hearing to a data controller's arguments that these intrusive kinds of data processing are a "legitimate interest" of the data controller, or that proper consent with lengthy privacy policies has been obtained, or that they are necessary for "fulfilling the terms of an agreement". Any resulting privacy harm would be regarded as "collateral damage", necessary to achieve the primary, more important goal.

Finally, the desire of national governments to gather intelligence has lured them into a pragmatic, extensive and largely secret partnership with interests whose concern is not the public good but private profit or personal advancement [Pasquale F., 2015: 47]. Considerations of "national security" usually override those of human rights, and a DPA may have no say in balancing those concerns or else advocate the policy that the government told it to promote, even if the DPA is formally independent from the government.

The logical extension of that way of designing data protection legislation would be turn it into a mere set of administrative rules that channel the flow of personal data. The law's core purpose of protecting the fundamental human right to privacy through protecting data would vanish.

2.2. Underenforcement of personal data protection legislation by underresourced DPAs resulting in underprotection of individuals

The lack of effective remedies available to data subjects themselves makes them indifferent to protecting their privacy and rights, and as a result the rights of data subjects become degraded. Data subjects must lodge a complaint with a DPA in order to protect their interests, and the DPA's resources are not unlimited. It is not possible to review and investigate each complaint and to punish every violation of data protection regulations. The headlines in the media about fines levied on data controllers are a drop in the sea of overall non-compliance by data controllers that consider themselves out of the reach of DPAs or under their radars. This means that a huge number of violations remains unaddressed, which in turn substantial-

ly diminishes the motivation of data controllers to implement the necessary data protection measures. The hope that violations will go unnoticed is too alluring. If data subjects had an effective remedy to directly deploy against data controllers, it would greatly augment the efforts of DPAs and increase the cost of non-compliance for data controllers so that they would make an attempt in good faith to comply with data protection regulations.

Something is needed to reach a better balance between individuals and data controllers. The argument usually made against improving the balance starts from the claim that private organizations have an insatiable appetite for data and hinges on faith in the usefulness of ever-increasing data to inform decision-making and make it more effective. Individuals are losing this tug of war. Data protection law has been labelled a "dead letter" because legislation and judicial decisions are allegedly having only a marginal effect on data protection practices [Rule J., 2007: 192]. While introducing more effective remedies available to data subjects will not by itself change this trend, it may place some extra weight on the scale in favor of individuals. It may add a qualification to the current jape, "If the product is free, you are the product," and turn it into, "If the product is free, you are the product unless you have a weapon impossible to ignore at your disposal."

Administrative fines and DPA crackdowns cannot replace the initiative of individuals in protecting their own privacy interests. Apart from any of the other previously mentioned factors, DPAs do not have the resources to uncover, investigate and address all the possible violations of data protection. An increase in the number of complaints submitted to DPAs will only aggravate this problem. For example, in Russia there has been a 44% increase in complaints from data subjects during the first half of 2019 compared to the same period in 2018[55].

Only individuals themselves, or a group of them backed by organizations specializing in privacy protection, may challenge this status quo. Perhaps the result would be disappointing, but again: "nobody made a greater mistake than he who did nothing because he could do only little."

In short, the current approach of saddling the data subject with the burden of proof for establishing specific damages and a causal link with a specific violation discourages claims, reduces private enforcement of data protection rights, and undermines the effectiveness of the data protection system.

[55] Available at: https://rkn.gov.ru/news/rsoc/news68534.htm?fbclid=IwAR30E519qNDsnR68XrgcwoCcrQpZ3_1KCX1zRD2hqsjBN5Z1gn_XDHQxQLY (accessed: 01.08.2020)

3. How to Fix it?

3.1. Statutory compensation as an alternative remedy

The foregoing analysis of Russian case law and some examples drawn from the case law of other countries shows that the main problem with the claims for compensation of data subjects is in proving that there was definite certain harm recognized by law and establishing a causal link between a violation and the harm. Other kinds of remedies, such as compensation for moral harm, also fail to adequately address the problem. Therefore, the most obvious improvement is to exclude definite harm and causation from the burden of proof.

Although this solution may at first seem simplistic and radical, considering some analogous situations should help us see how reasonable it is. And we do not need to go far to find them: the clearest analogy can be found in intellectual property law. To avoid having copyright owners go through the difficult exercise of determining the exact number of infringements and the possible causal links to harm, a special remedy was applied in many jurisdictions: statutory damages[56] or in the terminology of Russian law "compensation for violation of an exclusive right"[57]. According a study from 2013, twenty-four countries have adopted a remedy of this kind for copyright infringement[58].

Although some "prototypes" of statutory damages may be found in the legislation of the Russian Empire[59], statutory damages are an innovation that the United States has applied to copyright laws in the international arena, and it succeeded in exporting it to other countries through bilateral and multilateral treaties as well as by other means [Samuelson P., et al., 2013: 530][60]. The original rationale for statutory damages was typically that estab-

[56] 17 United States Code §504 Remedies for infringement: Damages and profits.

[57] Art. 1252(3) of the Civil Code of the Russian Federation.

[58] Azerbaijan, Bahamas, Bahrain, Belarus, Bulgaria, Canada, China, Costa Rica, Dominican Republican, Israel, Kazakhstan, Kyrgyzstan, Liberia, Lithuania, Malaysia, Morocco, the Republic of Korea, the Republic of Moldova, the Russian Federation, Singapore, Sri Lanka, Ukraine, the United States, and Vietnam. The authors of the study points out that the United States is in strange company here.

[59] According to Art. 23 of the 1911 Law on Copyright of the Russian Empire, a copyright owner is entitled to claim damages for infringement, the amount of which is defined by the court in accordance with the requirements of fairness.

[60] Available at: https://cyber.harvard.edu/people/tfisher/IP/Samuelson_SDs_2013.pdf (accessed: 01.08.2020)

lishing the number of copies that had been made by an underground pirate publisher would be difficult and that awards of statutory damages would save rights holders from having to do so. Statutory damages are an atypical ("extraordinary") remedy mainly because they allow owners of rights to recover substantial monetary damages within a fixed range of amounts without any proof that the plaintiff suffered any actual harm from the infringement or that the defendant profited from the infringement. According to US copyright law, these damages can be awarded in whatever amount the judge or jury deems "just" within a range between US $750 and US $30,000 per infringed work, and up to US$150,000 per work if the infringement is willful. Under Russian law the range is between 10,000 and 5,000,000 rubles (approximately, US$150 to US$80,000 per infringed work). If the statutory minimum seems out of proportion with the offense, awards less than the statutory minimum are possible, although this to a certain extent undermines the punitive purpose of this remedy[61].

Personal data and objects of copyright have many similarities. Both consist of *information*. Both copyright infringement and personal data violations may be treated as *misuse* of information. But the most important similarity between them is that *proof of damages* caused by misuse and of their exact amount *is extremely difficult* or even impossible, either because of the intangible nature of the damage, or because the claimant lacks the necessary information, or because the damage is remote from the actual misuse.

These similarities justify the application of similar remedies. If a new special type of remedy has been devised for copyright infringement in order to offset the ineffectiveness of the existing remedies, why can it not be applied also to cases in which the conventional remedies are ineffective and the object (information) is of the same kind? Furthermore, case law on copyright has already acknowledged its usefulness in protecting privacy interests [See for details: Samuelson P., 2013: 191–198].

That there are substantial difficulties in the definition of harm (damages) in data privacy cases and consequently for an individual to prove such harm has already been mentioned, and that problem has been thoroughly examined in legal literature. As a specialist in privacy issues and the internet observed in a US-based law journal, "A privacy harm must be 'cognizable,' 'actual', 'specific,' 'material,' 'fundamental' or 'special' before a court will

[61] Decree of Plenum of the Supreme Court of the Russian Federation "On application of part four of the Civil Code of the Russian Federation". 23 April 2019. No. 10.

consider awarding compensation. Leading commentators question whether privacy harm is much of a harm at all."[Calo R., 2011: 1132]. The author of a book on EU data protection law argues that "it is not possible to develop an exhaustive taxonomy of harms caused by unregulated data processing." [Lynskey O., 2015: 211].

The peculiar nature of privacy harms is recognized in case law as well. The European Court of Justices alluded to it specifically in its *Digital Rights Ireland Ltd* v *Minister for Communications* judgement, which found that personal data processing may have a chilling effect on individual behavior because it gives individuals the impression that they are being surveilled or monitored; and that in turn has both an inhibiting and a controlling effect on them. The current ubiquity of information technology, as well as the ability use it to aggregate the data gathered, has blurred the lines between information gathering and surveillance [Austin L., 2003: 119, 151]. Some scholars have even coined the term "dataveillance" for this topic, which they define as "the systematic use of personal data systems in investigation or monitoring the actions or communications of one or more persons [Clarke R., 1991: 496]. Most courts operating within a conventionally established framework for damage compensation would not recognize a "chilling effect" as a legally significant harm, and the data subject would be denied just redress. Courts persuaded by the arguments of some authoritative scholars that human access to sensory or other personal information is a necessary condition for privacy harm and that processing alone, if never "displayed to a human," leads to "no adverse consequence of any sort" [Goldman, E., 2005: 228], would be even less inclined to provide that redress. In an article by a prominent US judge and author of books on invasion of privacy, there is this opinion that computer searches do not invade privacy because programs are not sentient beings." [Posner R., 2008: 254]. However, studies of automated decision making [Pasquale F., 2015:14; Keats D., 2008: 1249][62], which is becoming commonplace now, have pointed out the error here. The fact that much information processing now occurs outside human sensory and temporal awareness does not mean that it cannot lead to negative consequences and deprive person from protection, as

[62] "The success of individuals, businesses, and their products depends heavily on the synthesis of data and perceptions into reputation. In ever more settings, reputation is determined by secret algorithms processing inaccessible data. Few of us appreciate the extent of ambient surveillance, and fewer still have access either to its results — the all-important profiles that control so many aspects of our lives."

long as we continue to recognize that an unconscious patient in a hospital bed is entitled to the same suite of rights and level of privacy protection as that patient had when fully aware.

One solution would be to stretch the concept of damage to somehow accommodate this particular privacy-related type of harm. But this may distort the regulation of claims for damages in general and have unintended negative consequences for the legal system. It is also highly unlikely that the situation could be corrected merely through some guidelines issued by a supreme court or other authoritative body to the effect that the courts are to award more compensation for moral harm. That would not make it easier to ascertain the fact of moral harm and trace out a causal link between it and a violation. A better response would be to exclude any kind of damage from the burden of proof and create a new alternative remedy. This would also align with the established position of the ECHR, according to which "the applicant cannot be required to furnish any proof of the non-pecuniary damage he sustained"[63].

This alternative remedy could be named "statutory compensation for violation of the individual's data protection rights" or just "statutory compensation" to distinguish it from statutory damages for copyright infringement and other customary damage claims.

3.2. Human rights justification for statutory compensation

The right to personal data and its role in representation of a person in a digitalized world is fundamental to the exercise of freedom in digital society and managing one's digital identity. Manipulation with figures and data relating to the individual leads to manipulation of people. Conferring a remedy for violation of the individual's data protection rights on the individual and making it applicable even in the absence of tangible or intangible harm serves the general interest. That general interest is similar to the general interest in protecting liberty. One of the clearest illustrations of this thesis is in UK case law pertaining to the tort of false imprisonment. In *Murray* v *Minister of Defence* the House of Lords noted *obiter dictum* that neither consciousness of confinement nor proof of special damage was a necessary ingredient of the tort. Lord Griffiths emphasized that "the law attaches su-

[63] Artyomov v Russia, No. 14146/02, 27 May 2010, §218; Antipenkov v Russia, No. 33470/03, 15 October.2009 §82; Gridin v Russia, No. 4171/04, 1 June 2006, § 20.

preme importance to the liberty of the individual and if he suffers a wrongful interference with that liberty it should remain actionable even without proof of special damage"[64].

As legal scholars have commented, "there is a general interest in upholding individual liberty, which goes above and beyond the individual consequences"[65]. It is possible to draw an analogy here, as Orla Lynskey does, with personal data regulations because a similar general interest in granting individuals control over their personal data exists, irrespective of whether they suffered harm or not in a particular case [Lynskey O., 2015: 196]. Lynskey argues further that granting control to individuals over their personal data may constitute the latest step in the evolving expansion of the individual's sphere of control. In the past, individuals have been given control over their property or personality, and data protection legislation extends this individual control to encompass digital manifestation of personality[66]. Other scholars also have found similar analogies between personal data and other freedoms. For example, the philosopher Boudewijn de Bruin argues that processing personal data can result not merely in an immediate loss of freedom for an individual; it can also bring about a future loss of "negative freedom" — the freedom to act without external impediments [Boudewijn de Bruin, 2010: 505, 514]. This is especially true when personal data is used for profiling, which may lead to discrimination or automated decision-making with regard to an individual.

If we accept that control over personal data is the essence of the fundamental right to manage personal data and privacy, then we should also apply the principle of international law that an effective remedy should be attached to that right and accept that the remedy may become an important component of a data controller's accountability.

The ECJ underlines the special importance of private enforcement of data protection legislation because "legislation not providing for any possibility for an individual to pursue legal remedies…, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter"[67].

[64] Murray v Minister of Defence, 1998, 1 WLR 692.

[65] Markesinis and Deakin's Tort Law. Oxford, 2008, p. 465.

[66] Idem.

[67] Schrems v Data Protection Commissioner, Case C–362/14, 6 October 2015, para 95.

Some traces of this thinking may be found in the European Commission's claim mentioned earlier that the UK had not implemented Data Protection Directive of 1995 correctly because the UK Data Protection Act of 1998 did not provide for "moral damages". An extract from one of the sources mentioned by Court of Appeal of England and Wales speculates that the Commission's view is

> that "an effective remedy" must include some element of compensation for any breach (*emphasis added.* — A.S.) of the (Data Protection Act) and therefore where a breach has caused a hurt to feelings or dignity but no actual loss a remedy in damages should be provided by the UK courts. On the other hand, it can be strongly argued, that there is no such obligation as long as the domestic legal system provides an effective set of remedies[68].

3.3. Functions of statutory compensation

Introducing a new type of remedy for violation of data subjects' rights becomes especially attractive when we consider the functions which statutory damages play in the enforcement of copyright law and understand their relevance to data protection.

Paula Samuelson has outlined the following functions of statutory damages as: (1) a rough approximation of the compensation due for actual harm and/or profits lost; (2) a deterrent sufficiently large to discourage the defendant in a particular case from infringing again; (3) retribution for the defendant's misconduct; and (4) a general deterrent. The general deterrence rationale can be further separated into: (1) the general deterrent value in punishing defendants fairly, including retribution, in proportion to their own conduct and in such a way that other similarly situated potential defendants would fear being punished;, and (2) punishing defendants with an award beyond what their conduct individually merits in order to set an example that will deter the public at large [Samuelson P., 2013].

In Russian academic literature there is no common approach to the nature of statutory damages, whether punitive or compensatory, although there is an attempt in case law to reconcile them in practice [Starzhenetskiy V., 2015]. It seems that the Council of Europe's Modernized Convention No. 108 adopts a similar stance, according to which "in any event, any sanc-

[68] Google Inc v Vidal-Hall, para 70.

tions imposed need to be effective, proportionate and dissuasive"[69]. One interpretation could be that requiring the sanction to be proportionate refers to its role as compensation; that the requirement of dissuasiveness pertains to its punitive or deterrent function; and that meeting both requirements makes the sanction an effective one.

If there is anything about which regulators and data protection specialists agree, it is that protection of data subjects' rights and the overall level of enforcement of data protection regulations has much room for improvement. Underresourced DPAs and data subjects lacking effective remedies and motivation to protect their rights cannot facilitate effective enforcement, while data controllers have too little incentive to comply with data protection regulations voluntarily. Instead of making a sustained effort to comply with data protection regulations, many of them are erecting so-called Potemkin villages to give the illusion of compliance[70]. Introduction of a new remedy with a punitive element and administered in a decentralized way by data subjects may change the situation. Statutory damages may make data protection enforcement more uniform and successful.

This argument becomes even more persuasive in view of the conclusions reached by the EU FRA study on access to data protection remedies in the EU. It states that "financial compensation was not a motivating factor to seek redress… *they sought redress to ensure that similar data protection violations do not recur* [emphasis added]"[71]. In other words, the deterrent

[69] Explanatory Report to Convention of the Council of Europe No. 108+ (Convention for the protection of individuals with regard to the processing of personal data). 2018, p. 29. Available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (accessed: 01.08.2020)

[70] The term comes from reports of a fake portable village built solely to impress Empress Catherine II by her former lover Grigory Potemkin during her journey to Crimea in 1787. While modern historians claim accounts of this portable village are exaggerated, the original story was that Potemkin erected phony portable settlements along the banks of the Dnieper River in order to impress the Russian Empress; the structures would be disassembled after she passed and re-assembled farther along her route to be viewed again as if there were another settlement. This term is widely used in the US case law, e.g. in the 2018 lawsuit filed against Exxon for fraud relating to the discrepancy between the published cost of climate regulations and the internally calculated costs. New York Attorney General Underwood's complaint alleged, "Through its fraudulent scheme, Exxon in effect erected a Potemkin village to create the illusion that it had fully considered the risks of future climate change regulation and had factored those risks into its business operations." See: Summons and Complaint in *People of the State of New York* v *Exxon Mobil Corporation*, Supreme Court of New York, 24 October 2018, p. 11.

[71] EU FRA, Access to data protection remedies, p. 8. A high proportion of survey respondents wanted to minimize the risk that other individuals would become victims of data protection violations. They most frequently mentioned "prevention of future violations of rights", "awareness rais-

function is one of the features of the effective remedy most demanded by individuals. This becomes especially understandable once we realize that certain types of privacy damage cannot be remedied; unlawful disclosure and distribution of sensitive medical information would be one example. As patients' rights advocate Deborah Peel observes, "with consumer credit cards, it is possible to close accounts, terminate authorization, and reissue credit cards… breaches of electronic health records cannot be fixed, and privacy cannot be restored" [Peel D., 2015: 178].

3.4. Criteria for definition of appropriate amount of compensation

What criteria courts should apply in setting the appropriate amount of statutory compensation is one of the basic questions about how to implement it. Here again we can turn to many of the already established precedents in case law pertaining to copyright infringement. As one example, the following criteria taken from copyright infringement cases may be used as guidelines for data protection cases:

the scope of the infringement;

how long the infringement continued;

the severity of the infringement;

the actual injury caused to the claimant according to the assessment of the court;

the benefit derived by the defendant from the infringement, according to the assessment of the court;

the nature of the defendant's activity;

the nature of the relationship between the defendant and the claimant;

the good faith of the defendant.

Some of these criteria are already used by the courts in privacy-related disputes. For example, the Supreme Court of Korea outlined the following factors for assessment of circumstances under which mental distress arising from data leaks may be compensated even in the absence of pecuniary damage:

the type and characteristic of the personal information leaked;

whether a third party accessed the leaked information and, if not, whether there is a probability that a third party had such access or will have it in the future;

---

ing", "stopping the wrong practice", "standing up for fundamental rights", "teaching a lesson to concerned authorities", "obtaining an acknowledgement of the violation from a competent authority" or "imposing a sanction on the perpetrator" (p. 29).

to what extent the leaked information was disseminated;

whether the leak caused any additional infringement of rights;

the actual way in which personal information was managed by the defendant;

any specific circumstances in which the information was leaked;

what measures were taken to prevent injury caused by the leak and to prevent the dissemination of the information[72].

In other words, while maintaining the necessary degree of flexibility, it is possible to outline a number of factors which should be considered by courts in order to ensure some degree of uniformity and predictability in the application of statutory compensation for violations of data privacy rights.

The problem in applying statutory compensation to multiple violations of data subjects' rights committed by a data controller may be solved in different ways. The first approach would be to treat all violations undertaken as part of a single set of activities as a single infringement for the purposes of statutory damages. A second possibility would be to establish a cap on the overall award. Finally, there could be a cap which would apply in the absence of any evidence that the plaintiff's actual loss exceeded that amount. The first approach looks the most promising, at least while the new remedy is still in "test mode".

3.5. Not-for-profit organizations as the key player in enforcement of the new remedy

As was illustrated above, the costs, timing and overall efforts associated with protection of data subjects' rights in court proceedings are a substantial barrier to private enforcement of those rights. Lawyers and specialized organizations in many cases lack the financial motivation to engage in disputes of that kind.

[72] GS Caltex Data Breach Case, Supreme Court decision 2011Da59834,59858,59841. 26 December 2012. Available at: http://library.scourt.go.kr/jsp/html/decision/9-69%202012.12.26.2011Da59834.htm (accessed: 15.07.2020). Ultimately, the Court dismissed the claim on the ground that emotional distress cannot be assumed merely due to the existence of a large data spill. Either actual damage or emotional distress would have to be proven and shown to have been caused by the data spill. This is one more illustration in support of the position that effective remedies which empower data subjects to seek redress for violations of personal data regulations should be free from the requirement to prove the fact of privacy harm.

Article 80 of the GDPR provides an important foundation for bringing a new type of claimant to bear on privacy matters. It gives the data subject "the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data … to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."

According to the EU FRA, this would:

> enable civil society organisations and other bodies working in the data protection field, and having the necessary expertise and knowledge of the legal rules and situation in practice, to take a more direct role in litigation. This would in turn help to ensure better implementation of the data protection law, in particular where certain practices affect a multitude of individuals and/or where the victims of a breach of data protection rules are unlikely to bring individual actions against a data controller, given the costs, delays and burdens they would be exposed to. The introduction of broader legal standing rules would have to be done hand in hand with specific safeguards to preserve the fine balance between preventing abusive litigation and effective access to justice for data subjects[73].

But as this paper argues, these beneficial effects will appear only when accompanied by a new kind of remedy available to data subjects. That change may indeed bring about a kind of collective approach to enforcing data protection rights in the sense that a data subject is not left on their own in opposing a powerful data controller. This would provide an additional incentive for data controllers to take privacy commitments more seriously and put appropriate measures in place, especially if the activities of these institutions are followed by noticeable sanctions for any breaches of privacy.

To a certain extent this reform may also improve some long-standing problems with privacy policies. As Daniel Solove observes: 1) people do not read privacy policies; 2) if people read them, they do not understand them; 3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and 4) if people read them, understand them, and can make an informed choice, their choice might

[73] EU FRA, Access to data protection remedies, p. 32.

be skewed by various difficulties in reaching a decision [Solove D., 2013: 1881]. This exposes an interesting paradox explained by Omer Tene in a US-based law journal: "if information is simplified, individuals will not be fully informed; if information is detailed, individuals will not understand." [Tene O., 2013: 1246].

When a statutory compensation remedy is available, it creates an additional incentive for certain individuals to dig deeper into privacy policies accepted by them because it may result in a direct monetary reward. It also provides a financial motivation for active privacy activists and institutions that defend human rights and/or data subjects' rights to analyze and monitor compliance with them. This may breathe new life into privacy policies and the overall transparency of personal data processing.

3.6. The new remedy may be a strong weapon, but not a magic bullet

The new remedy cannot by itself address all the data protection problems which are often rooted in the limitations of human nature. Based on research in behavioral economics, cognitive sciences and human-computer interaction, arguments have been made that the complexity of data management matters is such that our judgments about it are prone to errors stemming from lack of information or computational ability, problems with self-control, and biased decision-making processes. For instance, time and attention are limited; it is impossible to control every single piece of information about oneself which circulates on the networks through myriads of channels and databases. Another consequence of the emphasis on active choosing or control is the difficulty raised by people's preference not to choose. Indeed, the costs imposed on data subjects can be so high in complex and technical areas they are unfamiliar with that the majority of them tend to stick with the default options instead of exercising their freedom of choice and being in control of the situation [Lazaro C., Le Métayer D., 2015: 32]. Lazaro and Le Métayer "believe that it is nearly impossible for data subjects to really measure the breadth of their disclosure and the long-term effects of their actions. It is thus very unlikely that they do not suffer harm even from a potentially informed, autonomous and responsible decision." Therefore, as Solove suggests, it is still necessary to "continue to engage in an elaborate dance with the tension between self-management and paternalism." [Solove D., 2013: 1990].

These complications do indeed substantially decrease the potential for active participation by most data subjects in defending their rights as data subjects. Nevertheless, introducing statutory compensation for data protection violations may become an important part of the overall enforcement of data protection regulations and management by individuals of their digital personae and reputations. It may prevent or at least slow down their commodification in the digital era. Ultimately, it may help to overcome the shortcomings from underenforcement of existing data protection regulations by the data subjects and underresourced DPAs.

References

Acquisti A. (2010) The Economics of Personal Data and Economics of Privacy. Paper presented at the OECD Round table, p. 26.

Austin L. (2003) Privacy and the Question of Technology. *Law and Philosophy*, no 22, pp. 119, 151, 196.

Bogdanova O.V. (2017) *Protection of Copyright with Civil Law Remedies.* Moscow: Ustitsinform, 211 p. (in Russian)

Calo R. (2011) The Boundaries of Privacy Harm. *Indiana Law Journal*, vol. 86, p. 1132.

Citron D. (2008) Technological Due Process. *Washington University Law Review*, vol. 85, p. 1249.

Clarke R. (1991) Information Technology and Dataveillance in: *Computerization and Controversy: Value conflicts and Social Choices*. Academic Press, p. 496.

Bruin B. (2010) The Liberal Value of Privacy. *Law and Philosophy*, no 29, pp. 505, 514.

Erdelevskiy A. (1999) *Compensation of Moral Harm: Analysis and Commentary on the Legislation and Case Law*. Moscow: VEK, p. 192 (in Russian)

Fried C. (1984) Privacy (A Moral Analysis) in: *Philosophical Dimensions of Privacy*. F. Schoeman, ed. Cambridge: University Press, p. 209.

Goldman E. (2005) Data Mining and Attention Consumption in: *Privacy and Technologies of Identity*. K. Strandburg & D. Raicu, eds. Boston, MA: Springer, p. 228.

Greenleaf G. (2014) *Asian Data Privacy Laws: Trade and Human Rights Perspectives*. Oxford: University Press, pp. 115, 132, 151, 268, 283, 313, 519.

Kuner C., Bygrave L. et al (2020) *The EU General Data Protection Regulation: A Commentary.* Oxford: University Press, p. 1135.

Kuner C. (2013) *Transborder Data Flows and Data Privacy Law*. Oxford: University Press, pp. 30 ff.

Lazaro C., Le Métayer D. (2015) Control over Personal Data: True Remedy or Fairy Tale? *SCRIPTed*, vol. 1, pp. 10, 32.

Lynskey O. (2015) *The Foundations of EU Data Protection Law*. Oxford: University Press, pp. 196, 209, 211.

Marchenko S.V. et al (2004) Compensation for moral harm in the mirror of Russian law, *Advokatskaya praktika*, no 5, pp. 20–23 (in Russian)

O'Dell E. (2017) Compensation for Breach of the General Data Protection Regulation. *Dublin University Law Journal,* vol. 1, p. 3.

Pasquale F. (2015) Privacy, Autonomy, and Internet Platforms in: *Privacy in the Modern Age: The Search for Solutions*. M. Rotenberg et al, eds. New York: New Press, pp. 14, 166.

Pasquale F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, p. 47.

Peel D. (2015) The Future of Health Privacy in: *Privacy in the Modern Age: The Search for Solutions*, p. 178.

Posner R. (2008) Privacy, Surveillance, and Law. *University of Chicago Law Review*, vol. 1, p. 254.

Rule J. (2007) *Privacy in Peril: How We are Sacrificing a Fundamental Rights in Exchange for Security and Convenience*. Oxford: University Press, p. 192.

Samuelson P. et al (2013) Statutory Damages: A Rarity in Copyright Laws Internationally, But for How Long? Berkeley Public Law Research Paper No. 2240569, pp. 191–198, 530.

Solove D. (2013) Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, no 126, pp. 1881, 1888, 1900.

Starzhenetskiy V. (2015) Statutory Damages in the Intellectual Property Law of the Russian Federation. *Vestnik ekonomicheskogo pravosudia*, no 10, pp. 116–147 (in Russian)

Tabunschikov A.T. (2017) *Compensation of Moral Harm.* Moscow: Prospect, p. 29 (in Russian)

Tene O. (2013) Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws. *Ohio State Law Journal*, no 74, p. 1246.

Truli E. (2017) The General Data Protection Regulation and Civil Liability in: M. Bakhoum et al , eds. *Personal Data in Competition, Consumer Protection and Intellectual Property Law — Towards a Holistic Approach?* New York: Springer, p. 312.

Von Bar C., Clive E., et al (2009) *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference*. Munich, pp. 3040, 3052.

Westin A. (1967) *Privacy and Freedom*. Toronto: McClelland and Stewart, p. 7.

Ylan Q. Mui (2011) Little-Known Firms Tracking Data Used in Credit Scores. *Washington Post*, July 16.