Legal Issues in the Digital Age, 2022, №4, С. 34-51 https://doi.org/10.17323/2713-2749.2022.4.34.51
Опубликована: Дек. 14, 2022

The Right to Informational Self-Determination: On the Edge of Public and Private

Talapina Elvira Vladimirovna
Russian Presidential Academy of National Economy and Public Administration, 82 Vernadskogo Ave., Moscow 119571, Russia, talapina@mail.ru, https://orcid.org/0000-0003-3395-3126

Аннотация

The right to informational self-determination, as the authority of the individual to decide fundamentally for herself, when and within what limits personal data may be disclosed, was formulated by German jurisprudence and has become a model for many States as well as for European Law in general. It is seen as a necessary tool for maintaining a vibrant democracy, on the basis that privacy is an “integral part” of society. The basis for the judicial decision was the Kantian theory of the moral autonomy of the individual. This explains the close connection of judicial reasoning with human rights and their Public Law protection. At the same time, under Anglo-Saxon influence, a “property approach” to personal data which may become the object of transactions is developing. The “property approach” views personal data as a valuable commodity that can be the object of transactions and operations with other people through licenses. In practice, access to personal data has recently been increasingly provided as a counter performance (compensation) to contracts for the provision of digital content and in exchange for personalized services. The study shows there are many interactions of public and private in the legal protection of data (information self-determination as a subjective public right requires the corresponding obligations of the State to be formalized, there is no unambiguous sector qualification of a person’s consent to data processing, the insufficiency of the principle of confidentiality by default before the potential for harm is noted). Analysis of the evolution of the data legal protection leads to conclude that the public/private distinction is gradually levelling off. It seems that the problem of the circulation and protection of personal data cannot be solved in a sector framework, but only comprehensively, without violating the traditional logic of public and private. This means that the right to information self-determination, due to its complex nature, can be regarded as a principle that has an inter-branch nature extends to

both the Public Law data protection and the implementation of subjective civil rights in this area.

Ключевые слова: personal data, human rights, privacy, confidentiality, digitalization, data treatment

Introduction

Issues of interpenetration of public and private law arise every minute, but conservative jurisprudence prefers to stay within the branch boundaries. Factors ‘diluting’ the boundary between public and private law in general, and between branches of public and private law in particular, have been growing in numbers, but the technology factor takes a prominent place: Digitalisation has begun to have a transformative effect on law. Digital technologies, neutral and universal by nature, ‘impose’ their own logic that levels off the boundary between the public and the private, sometimes causing conflicts with conventional legal routes.

A good theory is of crucial importance for proper and stable development of legislation in general, and for development in the area of information rights of individuals in particular [Arkhipov V.V., 2018: 52-68]. Moreover, this needs to be a well-balanced theory capable of identifying specific features of public law and private law regulators. Today, we need to define very clearly what personal data is, who owns it, how this data is protected and according to what regulations does liability for violations of rights in this area arise. Will this liability be under public law, or private law, or a combination of both of them? In any case, personal data are linked to a physical person, and oftentimes spread by this same individual. Does the ‘possession’ of personal data impose any obligations on a person? What are the boundaries between public and private interest in using personal data? What are the limits to which a person’s right to data extends? These and other questions are considered in this article, and the author proposes to regard it as an invitation to a discussion.

1. What is the Right to Self-Determination?

Present-day publications note integrative importance of the right to information self-determination in a system of new generation rights that include a range of rules related both to personal freedom and to digitalisation. Historically, information self-determination (Informationelle Selbst- bestimmung) was recognised as an independent right in a ruling of the German Federal Constitutional

Court[1], which has been extensively commented on in research publications, and not only in Germany.

The dispute centred on the 1983 Federal Census Act, which required the collection of a wide range of data pertaining to the demographic and social structure of Germany. The law established parameters for counting the country's population and required that personal information (name, address, gender, marital status, religious affiliation, occupation, place of work) be provided. The law also required people to answer questions about their sources of income, level of education, mode of travel to work, use of housing, including the way they heat and pay for utilities. Clearly, this information was collected not just for information's sake, but for further use (for planning purposes, environmental protection, etc.), and hence the law allowed the information collected to be passed on to local authorities. These could even compare the information they received with housing registers and adjust them, if necessary.

The provisions of this law became the subject of consideration by the German Federal Constitutional Court (hereinafter-Court). This decision has become a landmark both for the German legal doctrine and for the development of pan-European data protection regulations owing to its obvious and recognised influence on European legal thought.

It is noteworthy that the starting point of the Court's approach was the Kantian theory of the moral autonomy of the individual. This is significant because it explains the close relationship of the Court's reasoning with human rights and their public-law protection. Overall, the Court carried out a profound analysis of personal rights arising deep inside and penetrating various spheres including the information sphere.

As regards personal autonomy, the Court raised the concern that the collection, storage and use of personal information would threaten human freedom. The more you know about a person, the easier it is to control them. On the one hand, in today's information society, control over information means power, which the state seeks to obtain. But on the other hand, control over personal information is the power over one's own destiny, which is necessary to be able to freely open up and develop as a person.

This is why the Court has formulated the right to information self-determination as a kind of counterbalance to the information-

1. Decision of the First Senate of 15 December 1983. — 1 BvR209/83, 1 BvR269/83, 1 BvR362/83, 1 BvR420/83, 1 BvR440/83, 1 BvR484/83 // Selected decisions of the German Federal Constitutional Court. Moscow, 2018, pp. 75-86 (in Russ.)

gathering activities of the state. Information self-determination is an individual's right to decide when and to what extent their personal data may be disclosed. What is important is that this right was assessed not only retrospectively but also forward-looking: in the Court's view, technological development had already changed the possibilities for gathering information (it is worth reminding that the decision was made in 1983) and will change even more in the future. Indeed, in the past information was entered manually with the help of a punching machine and stored in separate locations, where only specialist staff had access. This made it difficult to obtain a 'portrait' of an individual by linking and combining different data (profiling). Today, almost anyone can enter and retrieve information electronically, which makes it easier to access instantly, and owing to big data technologies, personal information can be to extracted from seemingly unrelated data.

The Court ultimately upheld a large part of the challenged Act, although it did invalidate several provisions, including one that allowed local authorities to compare census data with local housing registers. The basis for such a decision was the possibility of combining these statistics, allowing officials to identify a specific person, thereby violating their rights as an individual.

The Court's reasoning appeared to be highly relevant in the context of separating public and private law. Human dignity, elevated to the top of the value structure, naturally extends to the entire legal system, i.e. both public and private law. Fundamental rights and corresponding duties are an essential part of human dignity [Eberle E., 2012: 224, 227-229].

It is worth noting that the concept of dignity is at the heart of the principle of individualism, which, together with the principle of equality, underlies modern constitutionalism. At the constitutional level, human dignity can be positioned as a principle of law that defines the purposes of or grounds for the adoption of the constitution, a specific human right or a permissible ground for limiting constitutionally recognised rights and freedoms [Vasilyeva T.A., 2020: 98-100].

It is worth mentioning that from a formal legal point of view, the right to information self-determination is not part of the Basic Law (Constitution) of Germany, but it is based on leading principles contained therein. While data protection is not mentioned in the Constitution either, the Court's ruling is based on Article 1.1 of the German Constitution, which states: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state

authority", in combination with Article 2.1 on self-determination "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." Proceeding from these two constitutional provisions, the Court held that the right guarantees a person's ability to determine whether his or her personal data can be disclosed and used. This became one of the first and best known wordings of the right to information self-determination.

The consequences of this milestone decision are significant both for Germany itself, where the principle of information self-determination has since consistently defended by the courts, for other states; e.g., Hungary has followed the German model [Szekely I., Vissy B., 2017: 137], and for European law in general. In Germany, this right is applied to protect quite a broad range of areas. "Designed to ensure a person's authority to make decisions on how others deal with their personal data, the right to information self-determination became a gage for verification whether the computerised suspect identification system, the video surveillance of an art monument located in the town square, the automated collection of vehicle licence plates, the obligations arising from the insurance contract when an insured event is established were in compliance with the Constitution." [Proskuryakova M.I., 2016: 84-98]. And the new European regulation (Regulation No 2016/679 of the European Parliament and of the EU Council 'On the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal
of Directive 95/46/EC (General Regulation on personal data protection)'), using the right to information self-determination, attempts to embed the right to protect personal data into the new digital economy by sharing with the owner the liability for his or her data that the state previously used to regulate. It is the digital challenges that, in our view, allow us to have a closer look at information self-determination, finding in it the potential for adaptation to the modern technology stage.

2. The Right to Self-Determination in the Digital Era

It is hard to argue with the forward-looking, pioneering nature of the court ruling made in 1983, for it did look to the future. That said, this ruling was for obvious reasons based on the data processing

technology development level at that time. And, probably, only George Orwell could have foreseen the current situation, where the unprecedented rates of data processing have given rise to a 'surveillance society.' The growing role of data, and transition from data gathering to data transformative use encourage legal discussions in various fields. The topics include the right to digital self-determination, divergent understanding of the ownership of personal data, and the state's protectionist stance on personal information expressed in increased public law protection of personal data.

This broad range coincides in many respects with the two dominant views on the impact of technology on the law as a whole. Supporters of libertarian views believe that the right to data protection may be alienated (sold), while egalitarian scholars lean towards the non-alienation principles, which are necessary to protect individuals from discrimination and stigmatisation, in particular in the socio-economic sphere. Consequently, the first position finds more support in private law and the second in public law.

2.1. Personal Data in Private Law

The personal data concept has its origin in the institution of privacy. The idea to protect privacy through law emerged in the 19th century, at a time when individualism was developing. The starting point for the right to 'informational privacy' is a classic essay by Warren and Brandeis published in 1890 in the Harvard Law Review, which compared the principle of privacy to the right to be left alone, "the right to opacity" [Warren S., Brandeis L., 1890:193-220]. The right to opacity protects an individual from being observed, scrutinised or spied on by others in their private sphere.

Following A. Westin's definition [Westin A., 1967: 7], US scholars have traditionally defined the right to privacy, or information confidentiality, as a right of individuals, groups of people, or institutions to independently decide when, how and to what extent information about them is shared with others. This has become the basis for the argument on the existence of an 'intangible property right' that everyone has over their personal data[2], and that people

2. The theory of 'property right' in respect of privacy has been initiated by supporters of economic analysis of law. In his analysis of confidentiality, Richard Pozner explained that a strong legal protection of privacy may result in negative economic consequences in the labour and loan markets. He believes the beneficiaries of privacy legislation will most likely be people with more arrests or convictions, or with a credit history worse than the average person

may lawfully ‘sell’ their personal data on the market thus choosing the best combination of confidentiality without state interference.

The ‘property approach’ regards data as a valuable commodity that can be the subject matter of transactions effected with other people through a license. In practical terms, access to personal data has recently been increasingly provided as a counter-performance (reimbursement) under contracts for the provision of digital content and in exchange for personalised services.

2.2. Developing a Public Law View

As opposed to the ‘information property’ theory, proponents of the public law approach point out that information as such does not exist until it is outwardly expressed or disclosed (i.e., information is always to a certain extent constructed.) Consequently, an individual cannot have ‘natural’, original rights to information or data related to this individual. In this sense, the German court’s decision that links information self-determination to the notion of dignity is interpreted as suggesting market inalienability of personal information by default. This view finds support in the attitude towards privacy as not only individual freedom but also an important element of a democracy (based on the assumption that private life is an ‘integral part’ of society): privacy and data protection are social structure tools for maintaining a free democratic society. Combining these messages culminates in the opinion that information, even if based on personality, is a reflection of social reality and cannot be related linked to a specific individual.

While data gathering aims to profile individuals, controlled persons do not have sufficient means to control such profiling themselves. At the same time, today, the ability to control and influence (in many respects, psychologically) the behaviour of individuals through data collection has increased dramatically. A person’s self-determination implies that individuals have the freedom to decide on their actions including the freedom to put their decisions into practice. And if a person cannot with a sufficient degree of certainty forecast what information about them in what areas is known to their social environment, and cannot assess with sufficient accuracy such awareness of the parties the communicate with, then this person is largely limited in their freedom to plan or make decisions without being subjected to any pressure. If, for instance, a person believes that participation in an assembly or other manifestation of civic initiative will be officially recorded and therefore there may be personal risks, this person may refuse to exercise the rights in

question. In the Court's logic, this affects not only the individual's chances of free development, but also the common good, since self-determination is an elementary functional condition of a free democratic society based on the capacity of its citizens to act and cooperate. And in general, privacy is more of a social structural imperative of democracy, since as a precondition of democratic discourse is that people feel free to express themselves without fear of being judged, without the possibility that state authorities could interpret their thoughts and behaviour based on the information gathered and processed. It is one of the responsibilities of the state in a democratic society to support and encourage the private and public expression of people's thoughts, preferences, opinions, and behaviour. In other words, privacy regimes and data protection regimes do not exist only to protect the interests of 'rights holders'. In a democratic society they are necessary to keep democracy alive [Rouvroy A., Poullet Y., 2009: 52, 57].

It is worth adding that the 1983 ruling of the Court views individual autonomy not as radical seclusion and independence of the individual in relation to their social environment, but as the autonomy of the individual who is included in society, lives and interacts with others. It turns out that technological development has bridged the gap between private and public law because not only an individual's personal development, but also the public good can be harmed. Incidentally, the idea of joint emergence and consolidation of private and public autonomy has been taken from Jurgen Habermas:"Valid, legitimate norms of action are only those with which all possible persons who would experience the consequences of accepting those norms would be able to agree as participants in a rational discourse" [Habermas J., 1995: 205]. From a legal perspective this means that individual autonomy, just like a musical or artistic talent, is something that the government would never be able to 'grant' to people through law. "The right to be autonomous' does not have any more sense than 'the right to be happy'" [Rouvroy A., Poullet Y., 2009: 59]. Interestingly, the right to seek happiness does exist in the legal reality (see the US Declaration of Independence).

Moreover, German scholars believe that the decisive argument for understating the right to information self-determination lies in the necessity to distinguish between the legal construct and the theoretical concept at the heart of the underlying law. Therefore, the construct of the right to information self-determination, which states that the processing of personal data by the state constitutes an

interference with an individual's right to determine the types and conditions of processing, is not an end in itself, but only a means to protect other basic rights. The theoretical concept here is this instrumental effect of the right to information self-determination. It is becoming increasingly evident from recent court practice that the German Constitutional Court does not interpret the right to information self- determination as strictly individualistic, but rather attaches a strong supra-individualistic dimension to it, which leads to objective demands regarding the processing of information by the state [Marsch N., 2020:40-41].

Such reasoning forms the basis for a regulatory data protection policy. As an objection to an individualistic interpretation of the right to information self-determination, experts emphasise that data protection legislation protects a whole range of interests, which cannot be regarded as a single legally protected commodity [Albers M., 2014: 213-235].

2.3. Automated decision-making

But online surveillance is not the only threat to individual self-determination. The functioning of automated decision-making systems also calls into question one's self-determination. From a functional point of view, it is essential that automated systems identify and analyse patterns of human behaviour at a level of depth and detail that was previously impossible, and that they can use these patterns to their advantage. Individual self-determination is threatened by the ever-increasing possibility for somebody else to understand a person's conscious or unconscious behaviour, and to openly or covertly use this knowledge in legal relations to improve their own position — for example by evaluating a person in an exchange of goods, services or information. In fact, this has always been the goal in business and social relations, but digitalisation is giving this process a new quality.

Opportunities for individual self-determination are impaired if the individual never knows what criteria the automated system uses. The literature defines this as insufficient clarity. Automated systems can identify people's characteristics, inclinations, goals and intentions in a previously unknown depth and detail and thus make predictions about their future behaviour. Human cognitive abilities cannot keep up with them, and so the human ability to actually comprehend the specific decision-making processes of automated systems reaches its limit. There is a danger that, if an automated system identifies a certain context and bases its decision on it, humans will no longer

understand the automated procedure. And if a person does not know which criteria the automated system uses, their capacity for individual self-determination, which is the basis of the entire human rights construct, is impaired.

In addition, the issue of legal significance of influencing people is of particular importance in legal terms. The main issue here is to determine when such potential for influence is legally significant and when, therefore, should the legal system treat it as a risk to individual self-determination? Basically, it is only the individual who can determine the intensity of the potential for influence. The level of perceived pressure aiming to change a person's behaviour largely depends on individual experience and can hardly be reduced to a particular type. The more personal data automated systems use to influence behaviour, the less transparent they seem, and so the more they influence a person's unconscious and irrational cognitive or intentional processes. The use of randomly appearing criteria can justify the prohibition of automated influences on individual self-determination (the use of criteria that are not predictable and understandable at the individual's current horizon of expectations) [Ernst C., 2020: 60,62].

It should also be borne in mind that many persons tend to coordinate their behaviour with the behaviour of others. For an individual the approval of the masses can make a certain decision credible, but it can also create an obstacle that would prevent deviating from that decision. Depending on the design of the decision-making system, there may be a concentration of behavioural patterns and a convergence of individuals. The number of options available to an individual may tend to reduce and focus on core behaviours and decisions. Then the realisation of individuality may require more efforts and expenses, and may even lead to social divisions.

These concerns are often cited as an argument for strengthening the right to information self-determination, both in public and private relations.

3. Mixed Interpenetration of the Public and the Private in Data Protection

3.1. Information self-determination as a public right

While the above views on the nature of personal data might seem diametrically opposed, this should not give the reader the wrong

idea. In actual fact, there is a lot of overlap in both the approach and the regulation of these issues. To some extent, the theory of subjective public rights emerged at the crossroads of public and civil law. Can the right for information self-determination be considered a subjective public right?

As LA. Pokrovsky wrote in 1917, after the collapse of the natural law doctrine, the positivist jurisprudence of the first half of the 19th century denied the grounds for constructing a person's subjective rights: The law protects life, physical integrity or honour of people, but there are no civil rights to life, freedom, etc. An individual's civil right only arises at the time a certain legal prohibition is breached and pertains only to the compensation of the losses incurred [Pokrovsky LA., 1998: 122]. And while an individual's interests (right to name, image, honour and dignity) penetrated civil law soon enough, the logic of protecting them originates from the logic of loss.

At the same time, in the same work of Pokrovsky we find that "civil law was originally and by its very nature the right of the individual human being, the sphere of his freedom and self-determination." [Pokrovsky LA., 1998: 309]. If we stick to the word 'self-determination', can we argue that information self-determination is one of these individual rights protected by civil law?

This question needs to be approached pragmatically, and the interests of the individuals themselves need to be taken into account. It is clear that quick and widespread technology development can result in the suppression of individuality. Qualifying information self-determination as a public right may ultimately prove more advantageous for people because, in addition to the subjective aspect of the rights that citizens can exercise, the objective aspect of the rights that they can claim from the government and its bodies are also assumed. This is the way the fundamental rights are in the constitution.

But even this may not be enough. In some jurisdictions, fundamental rights do not extend to the private sector, but in most cases constitutional provisions are binding on the private sector, too (which is to some extent a declaration, since private actors need substantive laws). In addition, it would be a good idea to equip the right to information self-determination with both criminal liability measures and civil redress mechanisms, i.e. to provide comprehensive protection.

3.2. Consent to personal data processing

The institution of consent to personal data processing has a significant role to play. Actions that would otherwise be illegal become legal through consent. It would be appropriate here to consider this problem from a geographic perspective (Europe — USA) and from a public/private perspective.

The EU has a some sort of paternalistic approach to data processing: EU law requires a much stricter and more explicit form of consent than US law. Moreover, EU law restricts the gathering, use and disclosure of data (a legal basis for personal data processing is required), whereas in the US, data can generally be processed unless the law specifically prohibits it.

This does not necessarily mean that more explicit EU consent requirements will necessarily lead to people undertaking a more meaningful cost benefit analysis of the collection and use of their data. But it takes more efforts and is more expensive to obtain consent under EU law. In today's world, the formal approach taken in EU regulations is rather a drawback because restrictions are often stipulated without any link to harm. As a result, regulation can prevent processing that does no harm and may even be beneficial. US law, on the contrary, usually permits data processing if it does not cause problems. [Solove D., 2013: 1900]. This situation has encouraged many researchers to take a closer look at the US approach owing to its flexibility and practicality.

Qualification of consent differs in public and private law. The civil law literature suggests that, by analogy with consent to the use of an image, consent to the processing of personal data should be treated as a transaction, and that as a result withdrawal of consent, the person who had the right to process such data could impose a civil penalty [Savelyev A.I., 2021:104].

Proceeding from a serious attitude to the fundamental principles of data protection and rejecting the 'information market' approach, public law scholars criticise the tendency to view individual consent as a sufficient criterion for the legitimacy of any kind of data processing [Rouvroy A., Poullet Y., 2009: 74]. They give an important role here to human rights, which ensure the autonomy of individuals in a free and democratic society. The classic' privacy and data protection regimes should be seen together as forming an evolving bundle of legal protection tools for the fundamental individual and social structural value of individuals' autonomous capabilities. At the same time, scholars propose to strengthen the right to information

and to grant new rights to consumers, including class actions, which again brings the issue to the intersection of the public and the private.

To outline the view of the Russian doctrine and practice on this issue, we would like to note Ruling of the Russian Federation Constitutional Court of 26 October 2017 No. 25-P "On the Case of Checking the Constitutionality of Article 2 Paragraph 5 of the Federal Law "On Information, Information Technologies and Information Protection" in connection with complaint of citizen A.I. Sushkov." This ruling attempts to evaluate a user agreement that assumes the existence of differentiated rules regarding access to user data. However, this attempt cannot be considered sufficient or successful.

3.3. Privacy by default or minimum harm?

The basic principle of data processing under the European Regulation (and, consequently, under Russian law, and even, to a certain extent, Chinese law[3], both of which follow European law in these matters), namely the principle of'privacy by design', makes it obligatory to process only the personal data that is necessary for each specific purpose of processing. However, data minimisation has been getting increasingly problematic and, given the growing proactivity of actors alongside with the collection of data in the process of total surveillance, hardly feasible at all. In view of this, the literature suggests that privacy by design' be transformed to 'minimum harm by design.' [Orru E., 2017: 107-137]. The difference between MHbD and PbD is that, firstly, it recognises that possible harm from surveillance goes beyond only violating privacy and attempting to provide guidance on how to remedy such violations; secondly, the burden of proof shifts to the surveillance parties. In essence, the proposal seeks to recognise the inevitable harm to privacy in the modern digital society and to respond to breaches in the general logic of civil law, with procedural preferences for holders of personal data.

The above issues provide a clear illustration of a real confusion between public and private law approaches to data protection, along with the state of incompleteness of legal protection of data.

3. See: Personal Information Protection Law of the People's Republic of China // Avai l-ableat: https://www.china-briefing.com/news/the-prc-personal-information-protec-tion-law-final-a-full-translation/ (accessed: 23.03.2022)

4. Data protection as a concept indifferent to the division of law into public and private

Based on an analysis of the evolution of data protection, scholars conclude that the public/private division has been gradually levelling off. E.g., in German law, the evolution of legal protection of personal data was mainly based on a hierarchical concept aimed at protecting the individual from the state. But following the establishment of personal data protection legislation, the traditional distinction between public and private law was challenged. This resulted in a unitary approach to regulation, regardless whether the data controller is a government agency or a private company. This is also true with respect to the European legislation on the protection of personal data. The new Regulation requires private data processors to balance their own interests with those of the individual whose data is processed. The Western literature regards this as “a most difficult and almost schizophrenic task”, especially for young companies and lawyers.

The US privacy law, on the other hand, largely attempts to increase individual freedom, including the commercialisation of personal facts (right of publicity) [Sattler A., 2018: 30, 36]. It also contributes little to division between the public and the private, which is not close to the Anglo-Saxon legal system in any case.

Thus, we have to note the erosion of the boundary between the public and private spheres. In these circumstances, the idea of data ownership is evolving, and this process is encouraged from both sides. Firstly, private law has been based on the principle of autonomy from the outset, thereby emphasising the freedom to act according to one’s will, so it is logical to give one the right to dispose of one’s data. Secondly, it pushes the development of technology. There is no need for in-depth research to prove that an individual’s consent to data processing, in the form of a check in the box on a website, bears little resemblance to informed and conscious consent as required by the European Regulation. Such consent has even been compared to a deal between an explorer and a native on a far-away shore in the sixteenth century, with the difference that access to personal data is exchanged for sparkling glass beads [Sattler A., 2018:40].

Certainly, the idea of personal data ownership seems attractive against this background. Since data has already become ‘the new oil’

and the process of data circulation is inevitable, it should be channelled in a civilised and regulated way. This has always been the legal logic.

However, a dive into the subject reveals a range of problems related to the fact that personal data, for obvious reasons, is not a subject matter of civil law and therefore the traditional civil law institutions simply do not focus on it. Let us recall that property in civil law can be linked to things (property right) and to intangible assets (intellectual property right). If a property right to personal data arises, it needs to be clearly defined. This is where the views differ significantly — should it be regarded as intangible good, as a subject matter of intellectual property rights, or as other property?

A.I. Savelyev characterises the evolution of the civil law definition of personal data as a gradual movement from personal non-property to property of a special kind, which falls under the category of other property under Article 128 of the Russian Civil Code. Civil law doctrine also raises the question of treating personal data as a counter-performance [Savelyev A.I., 2021: 129]. Of further note is the proposal to apply the relatively well-established regulations on intellectual property to Big Data [Sergeyev A.R, Tereshchenko T.A., 2018: 121]. This suggestion could well be applied to personal data.

International literature has also made references to copyright in this area and suggests some modification. A true empowerment of individuals whose data is processed can be made easier to attain by introducing a dualistic right. Such a right — in many ways similar to early copyright — can be a property right that allows the individuals in question to benefit economically from the use of their data. Here, suggestions are made to eliminate the inconsistencies between contract law, copyright and data protection law. At the same time, since personal information is diverse and highly context-sensitive, the right to personal data should (again by analogy with moral rights in early copyright law) be coordinated with due respect for human rights [Sattler A., 2018:48].

It seems that the problem of the processing and protection of personal data cannot be solved within a particular area, but only in a comprehensive way, without violating the traditional logic of public and private. Let us try to summarise the results.

In Lieu of a Conclusion

The right to information self-determination is at an intersection, of sorts, between public and private law, the challenges of new

technologies, and individual and public interests. It may well be that its successful resolution will serve as a model for building future legal regulation in a digitalised environment. We believe that the following needs to be taken into account.

Two approaches to the right to information self-determination are seen clearly. The original US approach to privacy self-management based on the notice and choice mechanism has been criticised in European doctrine as facilitating commercial exploitation of personal data and endangering user privacy, identity and dignity [Vivarelli A., 2020: 305]. In turn, Americans call the European approach excessively paternalistic [Solove D., 2013]. But despite their seeming polarity, these approaches can be combined, as long as we do not consider data protection to be solely a matter of private or public law.

The origin' of data protection from privacy protection has played a twofold role. On the one hand, the fact that private life was initially reflected in civil codes has placed its protection at the level of a civil right protected individually in the event of a violation. On the other hand, the increasing interference of the state in this area has created the basis for its constitutional recognition, following which data protection took on a life of its own. The rights to privacy and personal data, recognised as human rights, strengthen the public-law component.

No matter how it is defended, the right to information self-determination is not absolute and may be restricted in the public interest. From the personal data owner's point of view, this also outlines the limits of then-own responsibility because it cannot be left to the individual to determine the fate of the data. The state and its institutions have an important part to play, too.

It was long noted above different attitudes to information in public and private law: openness and privacy, respectively. Public law adds general guarantees by working through the institution of human rights, which acts as a guarantor of human-centred perspective in relation to the use of technology. At the same time, the growing tendency to apply civil law constructs in public law has an explanation: their resilience and stability have for centuries been successfully combined with flexibility and freedom, (relatively) independent of political change. What is also appealing about the civil law approach is that it is pragmatic.

The general context of modern governance, the focus on a social state and involvement of the private sector to public tasks, leads many jurisdictions to believe that a whole host of issues, including

data protection, are cross-sectoral and do not recognise the public/private distinction. Therefore the right to information self-determination can become a cross-sector principle that extends to both public data protection and the exercise of subjective civil rights. The comprehensive nature of this data protection principle involves building both public and civil law protection mechanisms combined with a subtle approach to the balance between their basic components.

References

1. Albers M. (2014) Realizing the complexity of data protection. In: Gutwirth 8., Leenes R. et al. (eds.). Reloading data protection: multidisciplinary insights and contemporary challenges. Dordrecht: Springer, pp. 213-235.
2. Arkhipov V.V. (2018) Personal Data as nonmaterial values (or there is nothing more practical than a good theory). Zakon=Statute, no. 2, pp. 52-68 (in Russ.)
3. Eberle E. (2012) Observations on the development of human dignity and personality in German constitutional law: an overview. Liverpool Law Review, 3, pp. 201-233.
4. Ernst C. (2020) Artificial intelligence and autonomy: self-determination in the age of automated systems. In: T Wischmeyer, T Rademacher (eds.) Regulating artificial intelligence. Cham: Springer, pp. 53-74.
5. Habermas Yu. (1995) Democracy. Reason. Moral. Moscow: Academia, 245 p. (in Russ.)
6. Marsch N. (2020) Artificial intelligence and the fundamental right to data protection: opening door for technological innovation and innovative protection. In: T. Wischmeyer, T. Rademacher (eds.). Regulating artificial intelligence, pp. 33-52.
7. Orru E. (2017) Minimum Harm by Design: Reworking privacy by design to mitigate the risks of surveillance. In: Leenes R. et al. (eds.) Data protection and privacy: (in)visibilities and infrastructures. Cham: Springer, pp.107-137.
8. Pokrovskiy I.A. (1998) Main issues of civil law. Moscow: Statut, 353 p. (in Russ.)
9. Rouvro A., Pou I let Y (2009) The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth S. et al.

(eds.) Reinventing data protection. Dordrecht: Springer, pp. 45-76.

10. Sattler A. (2018) From personality to property? Revisiting the fundamentals of the protection of personal data. In: Bakhoum M. et al. (eds.) Personal data in competition, consumer protection and intellectual property law: towards a holistic approach? Heidelberg: Springer, pp. 27-54.
11. Savelyev A. I. (2021) Civil law aspects of commercialization of personal data. Vestnik grazhdanskogo prava-Civil Law Herald, no. 4, pp. 104-129 (in Russ.)
12. Sergeev A. P, Tereshchenko TA. (2018) Big data: in search of a place in the civil law system. Zakon=Statute, no. 11, pp. 106-123 (in Russ.)
13. So love D. (2013) Privacy self-management and the consent dilemma. Harvard Law Review, v 126, pp. 1880-1903.
14. Szekely I., Vissy B. (2017) Exercising access rights in Hungary. In: C. Norris et al. (eds.) The unaccountable state of surveillance. Exercising access rights in Europe. Cham: Springer, pp. 135-180.
15. Um nova-Konyukhova I.A., Alferova E.V., Aleshkova I.A. (2021) Digital development and human rights. Moscow: INION, 174 p. (in Russ.)
16. Vivarelli A. (2020) The crisis of the right to informational self-determination. The Italian Law Journal, 6, no. 1, pp. 301 -319.
17. Warren S., Brandeis L. (1890) The right to privacy. Harvard Law Review, 5, pp. 193-220.
18. Westin A. (1967) Privacy and freedom. NewYork: Atheneum, 487 p.