ЮРИДИЧНІ НАУКИ

УДК 341.1/8
DOI: 10.15587/2313-8416.2016.75461

APPROACHES TOWARDS JUDICIAL AND SCIENTIFIC DEFINITION OF THE 'PERSONAL DATA PROTECTION' DISCIPLINE MAXIMS, THEIR EXPLANATORY AND CORRELATION

© A. Lytvynenko

The article deals with building up term explanatory from the discipline named "Personal Data Protection". The article is constructed on basis of Ukrainian legislation, the legislation of other states, international agreements as well as profile judicial literature. To fulfill the articles' goals, three terms were extracted from the notion compound
***Keywords**: personal data, data protection, ETS 108, OECD, HEW Report, explanatory*

У статті проаналізовано та витлумачено деякі терміни з понятійного апарату дисципліни «Захист персональних даних» на основі Законів України, законів інших держав, міжнародних договорів та юридичної літератури. Задля цього обрано 3 терміни – «недоторканність особистого життя (у розумінні персональних даних)», «персональні дані» та «обробка (опрацювання даних)»
***Ключові слова:** персональні дані, захист персональних даних, ETS 108, HEW Report*

1. Introduction

The juridical and scientific fidelity of the notions, which constitute the "Personal Data" and "Personal Data Protection" disciplines' conceptual vehicle, remains sufficiently topical for the legal systems of various states for over forty years owing to its' controversy and complexity of the basic notions. One has to keep in mind, that the legal regulations of data-related issues has got a blended germination, as its' main definitions were elaborated not only by lawyers, barristers and legal researchers (as Alan Westin, Pierre Juvigne), but also by technicians, being plurally lawyers or legal researchers (Arthur Miller, Lance Hoffman). The personal data-related issues are comparatively contemporary, as their scientific basement appeared only in mid 1960s in engineer and lawyer treatises, whose works were heavily impacted by colossal computing devices evolvement (the so-called "mainframes", relative databases, databanks (which were also designated as "data centers" before 1967)). Moreover, the 60's legislation did not regulate any data processing procedures. The same is equitable to say about international agreements.

2. Literature review

The personal data-related conceptual vehicle themes were worked out by multiple Western authors, including Alan Westin [1]. Kalvin Gotlieb and Alan Borodin [2], Colin Bennett [3] and Gloria Gonzalez Fuster [4]. One of the most prominent conceptual vehicle pioneers was a book by Willis Ware [5], which is also widely known in its' shortened version (a.k.a *HEW Report*), in which the author has elaborated a strong conceptual fundament, including the rights of data subjects, the rights and commitments of data controllers, technicians and data managers, data-maintaining requirements regarding the agencies, technical equipment etc [5, 6]. This book had a huge impact on OECD's "Guidelines on Data Protection…" (1980) and was considered by Council of Europe while developing the pilot Resolutions, namely the 73 (22) and 74 (29), released in 1973 and 1974 appropriately, as well as working out the ETS 108 (1981) Convention [7].

Unfortunately, Ukrainian scholars and legal researchers paid considerably less attention to the data protection conceptual vehicle, preferring to keep up to various practical aspects, or mostly combining the definitive vehicle with national legislation. One of these includes a collateral monograph by Bem, Horodyskiy, Satton and Rodionenko, which is a manual for law faculty students. However, this treatise has got an entirely practical vector, and the definitive vehicle is mostly associated with domestic law [8]. Thereupon, the aforementioned researchers, using a sideman released one more treatise, namely "*Media, conflict and personal data protection*" (2016). This manual was generally oriented on an off-site topic, but gave a handful of definitive vehicle explanatory. Unfortunately, within assembling this manual, the authors made several faults (but still the manual has got some good notions, too), which are analyzed and explained by the article's author in this article [9]. Among the other Ukrainian-language sources, the author would like to hallmark a comment on the Ukrainian law "On personal

data protection" by *Igor Usenko*, a Ukraine's honored lawyer, where he criticizes the provisions for their non-perfection. The detailed law provision as well as assessment of their compliance to international standards, is conducted in the dissertation by the article's author.

Retracing to "*Media, conflict and data protection*" manual, the author would like to outline, that in order to enhance their theses, the authors frequently advert to case law – the practice of European Court of Human Rights (Strasbourg, France). The author's humble opinion goes as follows: such an approach is not exonerate enough to become a main source of theses verification, as case law (including the European Court of Human Rights practice), in contrast with statutory law, can not give out the definitions utterly within the prism of cases. The practice of US Supreme Court goes closer to this, in such cases, as "*Katz vs United States*" 389 U.S. 347 (1967) and some others [10, 11]. When referring to case law, one has to bear in mind that it's vital to consider the cases' topicality in the time it arose. Yes, the *Katz vs United States* case does contain topical issues as for 1967: the issue was evolved from the question of wiretapping warranty (the petitioner was making bets using state phone lines, which is prohibited by the *Interstate Wire Act 1961* and lodged the petition to US Supreme Court, finding the usage of contemporary tracking devices by special services as a Fourth Amendment infringement; see more regarding privacy and case law in the author's dissertation) using a bug, set up from the external side of the phone booth – quite a then-contemporary technology [10]. Unfortunately, the authors of "*Media, conflict and data protection*" did not consider this and used half of content to explain the practice of European Court of Human Rights, having crammed the manual with 20 cases for examples [9].

3. The treatise goals

This article is aimed at depicting a detailed conceptual vehicle explanatory and its legal background, based on international instruments and the domestic legislation of several states. The author vectors at elaborating custom notions, involving a complex "personal data" definition. As the discipline has got some myths and arguable theses in its structure, to *fulfill the goals*, the notions are supplied with broad legal and doctrinal explanatory and several popular myths are analyzed and contradicted.

4. Main body. **Defining data protection notions: the legal and doctrinal angles**

After having done the brief source analysis, we have to determine, what terms are to be involved in the discipline's conceptual vehicle. The author considers starting from defining the following notions: "privacy & right to privacy", "personal data and their types", "data processing" and others. Of course, the conceptual vehicle is too volumetric to fit in one article. Therefore, only the aforestated terms are analyzed and described in the article. Apart from a wholesome terminology digest from various angles, the author also contradicts faux statements, as an illustration of the fact, that multiple "personal data protection" discipline notions are frequently misunderstood and misinterpreted, involving ambiguous or totally incorrect statements.

At first, let us deal with one of the discipline's cornerstones: what is privacy (or "[personal] life privacy") regarding automated data processing? It's a quite a complicated issue, as there's no precise definition of it. Well, at least, Alan Westin coined several "privacy" definitions way back in 1967, giving them quite a broad description:

"… [Privacy is] the claim of individuals, groups of institutions to determine for themselves when, how and to what extent information about them communicated to others. Viewed on terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical of psychological means, either in a state of solitude of small-group intimacy or, when among larger groups, on a condition of anonymity of reserve…" [1].

In his works, Westin analyzed various privacy violations, involving the data banks, too. Though, any data processing issues were never precisely covered by him. The early 1970s sources mostly exploited Westin's concepts (including W. Ware's "*HEW Report*") [5]. Westin's definition was also used by a US Supreme Court judge in the case "*Katz vs. United States*" (1967) [10]. However, a determined attempt to redefine the notion was carried out by Willis Ware from Rand Corporation in his 1973 "*HEW Report*" [6]. "There have been many definitions of privacy… – writes *Ware* in the "short version" of the report – all of which contain the common element that personal data are bound to be disclosed and that the data subject should have some hand in deciding the nature and the extent of such disclosure." [6]. The "privacy" definition by Willis Ware in its' narrow sense as given in "short" and "long" HEW Report is quite complicated: "Personal privacy as it relates to personal data". The definition of "privacy" in its' narrow sense, which is featured in the HEW Report, is also quite complicated: "Personal privacy as it relates to personal data record-keeping must be understood in terms of a concept of mutuality: the organization that holds personal data, must not have complete control over it, conversely, neither may the data subject. Each has a stake seeing that the information is used properly". The author also amends the definition by the following statement: "[Maintaining] a record containing information about an individual in identifiable form must be governed by procedures that afford the individual to participate in deciding what the content of the record will be and what the disclosure and use will be made of identifiable information in it" [6]. Ware also suggests that any record-keeping which involves data processing, which is not regulated by legislation, will be proscribe as unfair practice unless the national legislation does not authorize recording, maintenance, etc. [6].

So, we can conclude, that the narrowed meaning of personal privacy regarding the record-keeping practices is a really complicated notion. Moreover, critical lack of sources and specialists, who dealt with it, substantially exaggerates the issue. It's interesting, that neither *ETS 108 Convention* (1981) nor the *OECD Guide-*

lines… (1980) do not define this term anyhow. Ukraine's legislation has nothing to respond, as art. 2 of Ukraine's Law "On personal data protection" also lacks it [12]. The US Data Privacy Act of 1974 (5 United States Code Section 552a), a United States federal law, takes this term evasively: under subsection (a) (4) of Section 2, it is regarded as "a personal and fundamental right, protected by the Constitution of the United States" [13].

Therefore, the *HEW Report* is likely to be the only source of a narrowed privacy definition in the context of "Personal data protection discipline". We also would like to add, that Article 301 of Ukraine's Civil Code, in regard with personal non-property rights, also declares everyone's right on personal life. It's ironic that p. 2 of Art. 301 of Ukraine's Civil Code represents one of Westin's theses, dated 1967 [1]. The author of Chapter 3 of the aforementioned mini-manual "*Media, conflict and personal data protection*" refers to Art. 301 of Ukraine's Civil Code as one of the bases of "data protection" legal regulation, however, unfortunately, the Civil Code of Ukraine has nothing to do with it [14].

Tracing back to the foregoing topic, there's one more detail that should be tested within defining the "privacy" notion. We are to assure the reader that myths exist not only in literature or computer games, but in jurisprudence, too. The gist of this myth lies in the following: international agreements, as the *ECHR* or *UDHR* do really protect one's right to privacy. There are surprisingly two answers we are going to present: both "yes" and "no". Let us observe both approaches:

1. "YES": The right to one's privacy is proclaimed in Article 12 UDHR, Article 8 (1,2) ECHR and paragraph 1 of Article 17 ICCPR. These provisions are referred to in paragraph 11 of the "OECD Guidelines" explanatory report. But one could easily get the formality of such a treatment from paragraph 12 of the explanatory report, which is cited as follows: "However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions" [15].

2. "NO": The aforegiven provisions are treated tremendously broadly. Do not forget their timeline, which is 1948 for *UDHR*, 1950 for *ECHR* and 1966 for *ICCPR*. Taking into account that the privacy notion within record-keeping started to arise in mid-late 1960s, these provisions could hardly contain any connexion with "Personal data protection" discipline. The case law in the practice of European Court of Human Rights could cast light on Article 8 of ECHR explanatory, but citing Gloria Fuster monograph, the Court avoided any explanatory regarding Article 8, including the scope of the "privacy" concept; moreover, the Court nearly never dealt with it for almost 20 years before spring 1967, when studies regarding privacy and electronic techniques were initiated in the CoE expert groups [10]. After having conducted a two-year research regarding this topic, in 1970 the CoE Committee of Experts on Human Rights concluded that Article 8 of ECHR can not utterly protect one's right to privacy, which applies to data banks and record-keeping practices. Several statements of the conclusion are featured in CoE Resolution 73 (22) explanatory report and the CoE Yearbook of 1970. These Committees' ideas are also brought up in the authors' dissertation [16].

The "older generation" authors, Kalvin Gotlieb and Alan Borodin (1973) treat the aforegiven convention provisions quite skeptically, too. They consider such provisions are ambiguous, that's why they tend to treat the national legislation acts as the best privacy source regarding a certain state [2]. Willis Ware and other "*HEW Report*" authors consider that lodging amendments to the constitution (they naturally meant the United States, but this statement could be transposed to any other state) in regard with privacy protection also can not provide necessary safeguards [5]. According to Ware, these components are the following: 1) a well-elaborated data protection law 2) an overlook institution with substantial authority, illustrating it as "an independent, centralized Federal agency to regulate the use of all automated data banks" by giving registry and licensing to organizations, which maintain and exploit personal data. The shortened *HEW Report* version proposes a so-called "*ombudsman approach*", that is engaging an Ombudsman (a plenipotentiary for human rights) as a mechanism for regulation, which derives from Scandinavian countries. Willis Ware supports the "ombudsman approach" in the long "HEW Report" version, but emphasizes that it's efficient only in case appropriate legislation and procedures are already adopted [5, 6]. We would also like to hallmark that the "fathers" of the discipline conceptual vehicle, as Alan Westin and Pierre Juvigne, or Lance Hoffman and Paul Baran within their own explanatory never refer to any international agreements. Willis Ware also avoids it in his "HEW Report".

The conclusion and supplementing commentary from the analysis: while the author proactively supports the "NO" angle, perhaps nobody currently can explicitly answer this question. Yes, scholars, who tend to operate with an international law discipline named "*Human Rights*", would uphold the "YES" angle, but the author of this article has adduced enough statements to withstand it. What as to Ukrainian researchers, their position can be analyzed separately. So, the authors of the "*Media, conflict and data protection*" manual did neither delineate any "privacy" genesis notes, nor depict any of its definitions or elaborate a new one. Subsequently, it demonstrates the superficiality of this textbook one more time [9]. The authors of the manual named "*Personal data protection: legal regulation and practical aspects*" (2015) gave a more substantial position preferring to explain the notion generically exploiting the principle "YES", referring to the aforegiven provisions of international instruments. As mentioned before, they also appealed to case law in the practice of the European Court of Human Rights [8].

The author recognizes a certain contribution of case law into the conceptual vehicle evolvement, but it's needless to count on case law as the heading source or treat it, as a foremost and determinative agent in it. In the "HEW Report", Willis Ware emphatically discards case law, as a source: "[…] Nor should we look to court decisions to develop such general rules. Courts can only decide particular cases; their opportunity to establish

legal principle is limited by the nature of litigation arising from controversies between parties…" [5] Willis Ware stresses there were several privacy violation-related incidents in US case law, but only a few of them were connected with data recording practices [5]. These notions are depicted in details within the dissertation, including the case analysis.

Therefore, it's apparent that the precedents, referred in the aforegiven treatises, do not establish any particularly fresh definitions, which are demanded by conceptual vehicle – a decision of European Court of Human Rights in every separate case is either to contradict a thesis regarding ECHR Article 8 scope in regard with personal data protection, or to uphold it. Considering the position of "HEW Report" authors, we can contend that the path, proposed by the authors of "*Media, conflict and data protection*" manual is literally erroneous.

The next node, which is to be examined, is the personal data concept itself. So, what is "personal data", and what are its' main pillars? There are two approaches to deal with: the first is to exploit notorious definitions, and the other is to encounter the sources, which impacted the international agreements. In this article, the author is to conduct a comparative research to obtain a four-dimension view. If we follow the international instruments one would notice they propose identical definitions. Yes, in compliance with paragraph "a" of Article 2 of ETS 108 and paragraph "b" of Article 1 of OECD Guidelines personal data means any information regarding an identified or identifiable person, which is designated as the "data subject". Paragraph 10 of Art. 2 of Ukraine's law "On personal data protection" reveals an analogical definition [12, 15, 17]. The author of the "*Media, conflict and data protection*" argues that this definition is "*…terse and distinct enough and exists in compliance with international approaches towards its analysis*", augmenting the thesis with a following statement: "*the definitions given in international and national documents generically coincide*" [12].

Let the aforegiven statement (marked out in italics) become the second myth to deal with. Luckily Ukrainian legislation doesn't know what precisely a *national document is*: a legislation act (law, bylaw, code, directive etc.), or whatever else. Taking the statement seriously, the reader is to be assured that it can be easily withstood provided the older-generation sources are the "fathers". First and foremost, the ETS 108 definition arises more questions than answers:

– If any conjectural information is basically whatever, one can claim that a Zippo lighter (precisely Zippo, not any other), which is used by someone named John Smith also applies to personal data? If not, what are the criteria of their collating?

– Who, or what techniques are exploited or are capable of distinguishing personal data, who and with what intension is going to perceive the personal data of the guy we mentioned in the previous paragraph?

Hence we are to state here, that an individual familiar with "personal data protection" discipline will comprehend it relatively sufficiently. But a demand in developing a detailed definition really does exist. HEW Report (1973) did not give any precise definitions for personal data mentioning it only as data, which are bound to be disclosed. Willis Ware also elaborated an imposing list of personal data features emphasizing on person's primordial right to manage any possible data dissemination regarding him. For details, check the author's dissertation [5, 6]. What is more, even the term "personal data" is not an abominable panacea itself: the long and shortened HEW Report (1973) versions also apply such terms as "*individual data*", "*public records*" and merely "*records*" [5, 6]. The definition in subsection (a) (4) of Section 3 of 5 USC 552a (Data Privacy Act of 1974) gives an exhaustive definition what is personal data, designating it plainly as "*records*":

"*The term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph…*" [13].

The author considers that such a broad and complex definition facilely blows away the definitions given in paragraph "a" of Article 2 of ETS 108 Convention, as well as the hypotheses of "*Media, conflict and personal data protection*" authors as for a) term convenience b) coincidence with international approaches (incidentally they gave literally a zero of such approaches). [19 Besides, another statement regarding a definition coincidence between the OECD Guidelines and the 108th CoE Convention is also infidel, as the texts of both instruments were prepared by the two organizations starting from year 1976 with a large allotment of mutual collaboration, which is approved by multiple western legal researchers' monographs (e.g. Gloria Fuster, Eleni Costa), as well as the ETS 108 explanatory report [4].

The definition, given in subsection 1 of Section 1 of British Data Protection Act 1998 (Chapter 29) is slightly different from the one given in the American federal law:

"*… "personal data" means data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual…*" [18].

The Ukraine's legislation does not specify a profound personal data category list and what data should or shouldn't be considered as personal. Yes, in compliance with the Explanatory of Ukraine's Ministry of Justice from December 21, 2011 "On certain questions regarding Ukraine's law "On personal data protection" practical application", which elucidates its provisions and definitions, the law "On personal data protection", does not imply and does not set up a compound categorization of data regarding an individual which is meant to be personal data "owing to changes in technological, social, economical and other branches of social life" [19]. Hence the quantity of situations demanding any personal data exploitation or processing, as well as utter categorization

is seemingly larger than a sole definition can imply though it does not cancel the need to define it more broadly.

So we can conclude, that the approaches to define the notion do not coincide at all, having substantiated divergences instead. We could also conduct a discussion on the recognition capability regarding people or machines and their peculiarities, e.g. within ID numbers or other techniques, but let this dispute be abandoned for the dissertation treatise, as Alan Westin's concepts and Ware's "*HEW Report*" possess too much to tell to augment the conceptual vehicle just to imply it in the article; even case law has something to forward in it. Lastly, we'd like to accentuate the focus on our *pets*: the data which is maintained in state animal registries is nothing else but personal data. Taking into account Ukraine's legislation, there's a great issue: in compliance with point 1.4. of *Provision concerning the Sole State Animal Register*, approved by the *Decree of Ukraine's Ministry of Agrarian Policy and Foodstuff № 578 from September 25, 2012*, this registry contains over 20 data categories regarding birth date, ID documents, gender, colour, health status, transportation, etc., which are personal data, but belonging to an *animal* [20]. The author adverts to this statement within coining a new, complexified "personal data" definition.

Therefore, let us proceed to the last term to be depicted in this article, the "data processing", to be accurate. It is vastly connected with the operations, executed on personal data by empowered personnel. Keeping in mind the two previous cases, the term also contains an imperceptible myth that is also contradicted. To investigate the gist of "an overall work with personal data", let us present a definition, given in para. 8 of Article 2 of Ukraine's law "On personal data protection"

"Personal data processing is literally any action or a complex of actions, such as collection, registration, accumulation, storage, adaptation, alteration, revival, usage and dissemination (distribution, realization and transmission), depersonalization and personal data elimination, including within informational (automated) systems" [12].

Since OECD Guidelines do not lodge any definitions regarding this, let us switch to ETS 108, whose paragraph "c" of Article 2 gives quite a similar notion:

"[Automated data processing] includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" [17].

At first glance, the reader might guess there's no jive in it. But the myth itself is not on the surface, it's mounted in the vaults. In fact, the term "*processing*", which in Ukrainian is translated as "*обробка*" is initially a technical term, which refers to electronic computer operations. That is, the "processing" is executed by a computer, but the computer operator (an individual empowered to work with personal data, who is designated as "data processor" in the British Data Protection Act 1998, Chapter 29 in para. 1 of Section 1 [18]) only determines, what is required from the computer: storage, erasure of any other operation. Thus the term "data processing" regarding any data-related works arise scruple regarding the preciseness of the term. Such scruple could be easily confirmed with other definitions, but let us cite quite a non-trivial example to get the reader excited.

Let us represent a so-called "rheostat trolleybus theory". Having read such a subtle tagline the reader surmise what a term from a legal discipline and a rheostat trolleybus are supposed to possess in common? To throw in a bone, a trolleybus named MAN MPE-Sodomka-Siemens is a cybernetic model for the analysis, as it looks handsome enough to become one [21]. Trolleybuses do not possess a gearbox, and since the traction motor has got a high starting torque, there's a demand to fulfill smooth acceleration and braking. Therefore, the current intensity that flows through the motor coils is constrained by traction rheostats. The complex of techniques, which caters the trolleybus movement, is commonly called as rheostat-contactor powertrain, and the vehicles with it installed are apparently nicknamed as "rheostat".

This system has got three subtypes, but to comprehend the model only the most spread one is observed. The driver chooses what the trolleybus is to perform – to accelerate or to brake. The pedals are allied with the driver controller (here – the group traction rheostat controller), which is constructively a shaft that is operated by a high-voltage servomotor and within rotating it commutates the rheostats, handling the contactors with the help of lobes, which are engrafted onto the shaft [21].

Based on the "rheostat trolleybus" cybernetic model, I can depict the gist of personal data maintenance to the reader as follows: the operator addresses commands to the computer apparatus vectored at some action, as alteration, erasure, blocking, etc. But the processing is executed ingeniously by the computer, which is backed by the operator. Having the MAN MPE-Sodomka-Siemens trolleybus model in mind, we can't claim that the driver rotates the group traction rheostat controller by himself. Therefore, I can conclude that *processing* is an entirely technical part of *personal data maintenance* which convoys every its aspect, but it's *not* maintenance in generic sense. What is more, the term "processing" as a literal equivalent for Ukrainian word "*обробка*" hasn't always been in general use: yes, according to subsection (a) (3) of Section 3 5 USC 552a, the term "*maintenance*" is exploited to refer record-keeping practices, which meant storage, assemblage, use and dissemination. Para. 16 of CoE Resolution 73 (22) Explanatory report utilizes the term "*handle*", which referred to technical processing and storage, that is close to the aforegiven in the American federal law (5 USC 552a) [13, 16].

Tracing back to the treatises of the authors of "*Media, conflict and personal data protection*" manual, they input the definition in strict compliance with Ukraine's legislation. Taking into consideration they investigated the legitimacy of journalists' utilization of personal data in various situations, they somehow or other would bump into the defining problem, precisely, how to designate such actions. However they do not conduct any analysis on the rigour of the term and state as underwritten: «Hence, the dissemination of materials containing personal data by journalists is perceived as data processing according to the [Ukraine's] law» [9].

If we comprehend these statements literally there goes as underwritten:

a) Taking into consideration that modern websites contain personal data in any matter irrespective of the website genre, millions of earthlings do nothing else than *process data* and constantly exploit them?

b) If personal data could be maintained or worked with only by specially empowered personnel, hence, the actions of millions of individuals, who utilize them not having obtained a license or other authorization is deemed *illegal*?

Summing up the aforegiven theses, it's rectilinear to say that the claims of the authors of "*Media, conflict and personal data protection*" manual are nothing more than a clinical absurd. The subject that is meant to be "processing" is *exploitation*, which is absolutely legitimate according to point 2 of p. 2 of Article 25 of Ukraine's Law "On personal data protection", upon which data exploitation is allowed without applying the laws' provisions if it's utilized "…explicitly for journalist and creative purposes in case of preserving the balance between the right to privacy and the right to view expression" [12]. Thus the so-called *reductio ad absurdum* method used in aforegiven paragraphs "a" and "b" only asserts the thesis that any action upon personal data is erroneously regarded as *processing*; it's also likely to be called "*maintenance*" with technical processing. Therefore, the superior term has to be "*maintenance*" that involves all the working stages executed by authorized personnel. Every of its' constituents must involve technical processing. The personal data usage, as a "*maintenance*" particle is logical to designate as exploitation, as a citizen that exploits them is not empowered to conduct any specific works upon the data, but only to exploit, as a journalist or a scholar, etc. It's notable that the term "maintenance" ("опрацювання" in Ukrainian) was also proposed by a Ukrainian honored lawyer, Igor Usenko from *Kharkivska Pravozakhystna Grupa* (en. Kharkiv Remedial Group) as a substitute [22]. The author is to outline, that the authors' proposition to abjoint the terms in the Ukrainian law is not adopted from the comment of Mr. Usenko and derives from the rheostat trolleybus theory, which is used to elaborate new definitions for multiple terms as "*data processing*", "*data exploitation*", "*data maintenance*" etc. However, the contradiction of the third myth has stripped the fact that national legislation has got flaws regarding term definition, which are to be repaired by adopting amendments in the legislation.

A custom definition. In this article, the author proposes his own cognition view on the "personal data term". Hence the paragraph 10 of Article 2 of Ukraine's law "On data protection" is constructed to line as follows:

"Personal (or individual) data is a unit, a constellation or collection of data regarding a physical person or animal, registered in the Sole State Animal Register, that are withheld and encounter maintenance in appropriate agencies in compliance with acting legislation, which embrace, but are not confined with autobiographical records, education data, health status, property, financial transactions (involving tax payment), employment and self-employment, offence commitments etc. which contains the individuals' (or an animal's name, that is registered in Sole State Animal Register), a symbol, or another recognizing agent, owing to which, visually or viz various techniques the person (animal) could be ascertained; these methods include audiovisual means, as photographs and spectrograms and special ones – fingerprints, genetic information, etc."

The definition, mostly based on American federal law, is entirely custom, thus the reader can withstand it. This definition is obviously compound and too complex at first glance, but it actually 1) gives a narrow definetion 2) does not own ambiguities in contrast with more "terse" variants. The author deliberately does not use the term "identification" in the Ukrainian definition, as it's adopted from the English language and has enough national equivalents to cover it.

5. Results

To conclude, this is what the article was about:

1) The most complex conceptual vehicle terms were elaborated;

2) The myths regarding the three terms are contradicted and proved; typical faults are withstood and illustrated;

3) The definitions are given from various angles – that is Ukraine's and other states legislation, international instruments and juridical literature;

4) The role of case law regarding data protection principles and definition is assessed and analyzed;

5) The process of re-definition is invoked;

6) A custom "personal data" definition is coined;

7) Within formulating the disciplines' conceptual vehicle, the animal personal data are included in it, which is presumably the first overall time in its evolution history.

6. Conclusions

The article strips a problem of precise and high-grade explanatory of several terms from the "Personal data protection" conceptual vehicle based on the legislation of Ukraine, other states (USA, Great Britain), international instruments, Western juridical literature of "older" and "younger" generations. Three terms are widely observed – "privacy" (in the narrow meaning), "personal data" and "data processing". All of them do not possess ultimate definitions, and thus are often misunderstood or comprehended ambiguously; the acting definitions are presumably imperfect. The problem of their explanatory and treatment is amplified by the authors who are deemed incompetent, which is fully depicted in the article.

Nota bene. Please take into consideration that all the names of Ukrainian legal acts are given in English, being a verbatim translation from Ukrainian. To browse their original names, please follow the references. The author would also like to stress that all concepts and notions are explained entirely subjectively. The reader is free to object them.

References

1. International Social Science Journal – The Protection of Privacy [Electronic resource]. – UNESCO/UNESDOC. – 1972. – Vol. XXIV, Issue 3. – 237 p. – Available at: http://unesdoc.unesco.org/images/0000/000025/002559eo.pdf

2. Gotlieb, K. Social issues in Computing [Text] / K. Gotlieb, A. Borodin. – New York: Academic Press, Inc. (Elsevier), 1973. – P. 75–76.

3. Bennett, C. Regulating Privacy: Data Protection and Public Policy in Europe and the United States [Text] / C. Bennett. – Ithaka NY: Cornell University Press, 1992. – 288 p.

4. Fuster, G. G. The Emergence of Personal Data Protection as a Fundamental Right of the EU [Text] / G. G. Fuster. – Cham: Springer International Publishing, 2014. – P. 81–86.

5. Ware, W. Records, Computers and the Rights of Citizens [Electronic resource] / W. Ware // Justice.gov. – 1973. – Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

6. Ware, W. Records, Computers and the Rights of Citizens [Electronic resource] / W. Ware // Rand.org. – 1973. – Available at: http://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf

7. Thirty years after the OECD Privacy Guidelines [Electronic resource]. – OECD. – 2011. – Available at: http://www.oecd.org/sti/ieconomy/49710223.pdf

8. Bem, M. Personal data protection: legal regulation and practical aspects: a scientific and practical manual [Electronic resource] / M. Bem, I. Gorodis'kij, G. Satton, O. Rodionenko // Council of Europe. – 2015 – Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059920c

9. Bem, M. Media, conflict and data protection [Electronic resource] / M. Bem, I. Gorodis'kij, M. Levic'ka // MediaLab Online. – 2016. – Available at: http://medialab.online/wp-content/uploads/ 2016/04/1460489993222540.pdf

10. Katz vs. United States 389 U.S. 347 [Electronic resource]. – US Supreme Court (case law). – 1967. – Available at: https://supreme.justia.com/cases/federal/us/389/347/case.html

11. 18 U.S. Code, Chapter 50, Section 1084 (acting) [Electronic resource]. – Legal Information Institute. – 1994. – Available at: https://www.law.cornell.edu/uscode/text/18/1084

12. Ukraine's Law № 2297-17 from June 1, 2010 "On data protection" [Text]. – Verkhovna Rada Ukrainy (Ukraine's Parliament), 2010. – Available at: http://zakon3.rada.gov.ua/laws/show/2297-17

13. Title 5 USC Section 552a / Data Privacy Act of 1974 / Public Law 93-579 [Text]. – US Government Publishing Office, 1974. – Available at: https://www.gpo.gov/fdsys/ pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf

14. The Civil Code of Ukraine. Acting legislation with changes and amendments as for September 1, 2015 [Text]. – Kyiv: Palywoda A., 2015. – P. 107.

15. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [Electronic resource]. – OECD. – 2013. – Available at: http://www.oecd.org/sti/ ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

16. Council of Europe Resolution 73 (22). Text, annex and explanatory report. [Electronic resource]. – Ada.lt. – 1973. – Available at: https://www.ada.lt/images/cms/File/Resolution.73(22).doc

17. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Text]. – Council of Europe, 1981. – Available at: http://www.coe. int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

18. Data Protection Act [Electronic resource]. – Legislation.gov.uk. – 1998. – Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/1

19. Explanatory of Ukraine's Ministry of Justice from December 21, 2011 "On certain questions regarding Ukraine's law "On data protection" practical application". [Text]. – Verkhovna Rada Ukrainy (Ukraine's Parliament), 2011. – Available at: http://zakon3.rada.gov.ua/laws/show/n0076323-11

20. Decree of Ukraine's Ministry of Agrarian Policy and Foodstuff № 578 from September 25, 2012, approving the Provision concerning the Sole State Animal Register [Text]. – Verkhovna Rada Ukrainy (Ukraine's Parliament), 2012. – Available at: http://zakon5.rada.gov.ua/laws/show/z1713-12

21. MAN MPE-Sodomka-Siemens [Electronic resource]. – Imhd.sk. – 2012. – Available at: https://imhd.sk/ba/popis-typu-vozidla/26/MAN-MPE-Sodomka-Siemens

22. Usenko, I. Commentary on Ukraine's Law "On personal data protection" [Electronic resource] / I. Usenko // Kharkivska Pravozakhystna Grupa (Kharkiv Remedial Group). – 2012. – Available at: http://www.khpg.org/index.php?id=1330343937

References

1. International Social Science Journal – The Protection of Privacy (1972). UNESCO/UNESDOC, XXIV (3), 237. Available at: http://unesdoc.unesco.org/images/0000/000025/002559eo.pdf

2. Gotlieb, K., Borodin, A. (1973). Social issues in Computing. New York: Academic Press, Inc. (Elsevier), 75–76.

3. Bennett, C. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaka NY: Cornell University Press, 288.

4. Fuster, G. G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Cham: Springer International Publishing, 81–86.

5. Ware, W. (1973). Records, Computers and the Rights of Citizens. Justice.gov. Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf

6. Ware, W. (1973). Records, Computers and the Rights of Citizens. Rand.org. Available at: http://www.rand.org/content/dam/rand/pubs/papers/2008/P5077.pdf

7. Thirty years after the OECD Privacy Guidelines (2011). OECD. Available at: http://www.oecd. org/sti/ieconomy/49710223.pdf

8. Bem, M., Gorodis'kij, I., Satton, G., Rodionenko, O. (2015). Personal data protection: legal regulation and practical aspects: a scientific and practical manual. Council of Europe. Available at: https://rm.coe.int/CoERMPublicCommonSearch Services/DisplayDCTMContent?documentId=09000016 8059920c

9. Bem, M., Levic'ka, M. (2016). Media, conflict and data protection. MediaLab Online. Available at: http://medialab.online/wp-content/uploads/2016/04/1460489993222540.pdf

10. Katz vs. United States 389 U.S. 347 (1967). US Supreme Court (case law). Available at: https://supreme.justia.com/cases/federal/us/389/347/case.html

11. 18 U.S. Code, Chapter 50, Section 1084 (acting) (1994). Legal Information Institute. Available at: https://www.law.cornell.edu/uscode/text/18/1084

12. Ukraine's Law № 2297-17 from June 1, 2010 "On data protection" (2010). Verkhovna Rada Ukrainy (Ukraine's Parliament). Available at: http://zakon3.rada.gov.ua/laws/ show/2297-17

13. Title 5 USC Section 552a / Data Privacy Act of 1974 / Public Law 93-579 (1974). US Government Publishing Office. Available at: https://www.gpo.gov/fdsys/pkg/ STATUTE- 88/pdf/STATUTE-88-Pg1896.pdf

14. The Civil Code of Ukraine. Acting legislation with changes and amendments as for September 1, 2015 (2015). Kyiv: Palywoda A., 107.

15. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013). OECD. Available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm

16. Council of Europe Resolution 73 (22). Text, annex and explanatory report. (1973). Ada.lt. Available at: https://www.ada.lt/images/cms/File/Resolution.73(22).doc

17. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). Council of Europe. Available at: http://www.coe.int/en/web/ conventions/full-list/-/conventions/rms/0900001680078b37

18. Data Protection Act [Electronic resource]. – Legislation.gov.uk. – 1998. – Available at: http://www.legislation.gov.uk/ukpga/1998/29/section/1

19. Explanatory of Ukraine's Ministry of Justice from December 21, 2011 "On certain questions regarding Ukraine's law "On data protection" practical application". (2011). Verkhovna Rada Ukrainy (Ukraine's Parliament). Available at: http://zakon3.rada.gov.ua/laws/show/n0076323-11

20. Decree of Ukraine's Ministry of Agrarian Policy and Foodstuff № 578 from September 25, 2012, approving the Provision concerning the Sole State Animal Register (2012). Verkhovna Rada Ukrainy (Ukraine's Parliament). Available at: http://zakon5.rada.gov.ua/laws/show/z1713-12

21. MAN MPE-Sodomka-Siemens (2012). Imhd.sk. Available at: https://imhd.sk/ba/popis-typu-vozidla/26/MAN-MPE-Sodomka-Siemens

22. Usenko, I. (2012) Commentary on Ukraine's Law "On personal data protection". Kharkivska Pravozakhystna Grupa (Kharkiv Remedial Group). Available at: http://www.khpg.org/index.php?id=1330343937

Рекомендовано до публікації д-р юрид. наук, професор Макарчук В. С.
Дата надходження рукопису 08.07.2016

Lytvynenko Anatoliy, Department of International Law, Ivan Franko National University of Lviv, Universytetska str., 1, Lviv, Ukraine, 79000
E-mail: kenguru25@yandex.ru