Risks in the context of data protection

Martin Rost[1]

Abstract

The previous commentary literature on the Basic Data Protection Regulation (GDPR, see GDPR 2016) refers the term "data protection risk" predominantly to the avoidance of visible damage or loss of control for data subjects through the use of notoriously insecure IT. Such a narrowing of the understanding of the "riskbased approach" (RBA), however, loses sight of the encroachment on fundamental rights and the conditioning of the asymmetry of power between organisations and individuals.[2]

1 Introduction

Data protection is now often reduced to a protection of privacy and misunderstood. The urgency or dispensability of data protection thus becomes a question of personal values and preferences. However, data protection has a much broader function: in modern societies, it ensures that organisations do not undermine the existing expectations of autonomy, which are linked to various roles (e.g. as citizens, customers, patients). Such an understanding of data protection therefore also includes elements of statehood, such as the separation of powers, the rule of law and democracy, which on the one hand break the arbitrariness of organizations and on the other hand historically have allowed "the modern citizen" to emerge in the first place.

The way organisations - e.g. public authorities, companies, university institutes, associations, medical practices and notaries - deal with their internal and external staff in a modern society is one of the clearest indicators of damage to structurally necessary separations and separation of powers to protect against organisational arbitrariness. Organizational arbitrariness aims to turn dignified subjects into compliant objects. Arbitrariness finds its limits where

[1]This text is largely based on: "Rost, Martin 2018: Risiken im Datenschutz, in: vorgänge Nr. 221/222 (1-2/2018), S. 79-91", `http://www.humanistische-union.de/nc/publikationen/vorgaenge/online_artikel/online_artikel_detail/back/vorgaenge-221222/article/risiken-im-datenschutz/`

Martin Rost works as deputy head of the technical department of the Independent State Centre for Data Protection Schleswig-Holstein. He heads the sub-working group "Standard Data Protection Model" of the "Technology Working Group" (in German: "AK-Technik") of the Conference of Data Protection Officers of Germany. Contact: martinPOINTrostATmarokiPOINTde

[2]The translation of this text was largely done with the help of the great translation program deepl (`https://www.deepl.com`). I am aware that this text will therefore sound very German and contain some incomprehensible statements. I would be extraordinarily grateful for linguistic corrections by native speakers.

fundamental rights are recognised and enforced through supervision and effective sanctions, but not where only one market is enforced. Who belongs to an organisation and must expect a largely unsolicited evaluation and processing of their personal data? Who comes into contact with an organisation only occasionally, for example as a customer or citizen, and can expect a certain level of protection for their personal data? Deciding on these questions and shaping relationships is increasingly becoming a matter for the organizations themselves. It has been known since the 1970s that effective protection against organizational arbitrariness, whether by state or private bodies, is the central function of data protection. However, this knowledge has eroded in recent decades (cf. Pohle 2018). It is now very clear again that an operationally effective data protection system requires clear state and civil law sanctions.[3]

2 Risk

With regard to its selection and dimensioning of technical and organisational protective measures, the GDPR suggests an orientation towards risks. However, it would be wrong to speak of a "risk-based approach" to the basic regulation, as it is pursued, for example, in IT security. This term, which originates from the finance and insurance industries, is certainly not to be found in the GDPR.

The orientation towards risks should make it possible to transform the principles of data processing formulated abstractly in Article 5 as well as the provisions aiming at their implementation, effectiveness and verifiability (in particular Articles 24, 25, 32 and 35) into concrete processing and protective functions. The risk orientation follows the quite plausible idea that a data subject can feel concretely and directly at the occurrence or absence of damage whether the operative treatment of risks arising from a person-related processing activity has been successful or not. Recital (EC) 75 also recommends the use of the proven risk formula, according to which a direct risk for persons can be determined according to the formula "amount of damage multiplied by probability of occurrence". The application of this formula in data protection seems plausible, especially since it is part of the proven IT-Security-methodology of the Federal Office for Information Security (BSI), which determines the selection and intensity of the effectiveness of IT security protection measures. However, the BSI limits the benefit of this risk formula: "*Such extensive empirical values are missing in most cases in the very dynamic environment of information security. Therefore, in most cases it is more practicable to work with qualitative categories both for the frequency of occurrence and for the potential level of*

[3]Insurable risks can be included in prices. Non-quantifiable and therefore non-insurable risks, however, cannot be offset. An example of a civil law treatment could be a class action lawsuit system with the aim of an unpredictable and therefore uninsurable punitive damages, such as US-American damages.)

damage". (BSI 2017: 26) In other words, the risk formula is only suitable as a heuristic in the context of IT security.

In data protection, risks have been dealt with since the security of information technologies - first in the professional environment, later also in private use and in computer networks - became a relevant problem. In the meantime, the ongoing "computerization", "digitization" and "networking" of technical data protectors in particular have led to data protection risks being largely equated with IT risks (see Rost 2013). From the point of view of IT security, personal data is merely "data requiring special protection", which must be protected from unauthorized access (from the outside as well as from the inside). In many cases, even professional data protection professionals take the view that if IT is only operated with sufficient security and there is a legal basis for data processing, everything necessary in terms of fundamental rights has been done. From the point of view of data protection, such a view is not only too short-sighted, it is wrong. Establishing IT security is, of course, also indispensable for operational data protection. But this can only be the second step, before that there is the differently positioned task of reducing the encroachments on fundamental rights operationally to an unavoidable minimum. A few further remarks will follow shortly.

The technically narrow concept of data protection, which neglects the interests of third parties and the general public, is additionally reinforced by an economic perspective. According to this, the main problem to be solved for the data subjects or customers is to sell their personal data as expensively as possible to the companies interested in it: "*My data belong to me (and I determine their price)*". In this perception, the risk for the data subjects is that they sell their data too cheaply. If this bargain mentality does not turn into a fundamental understanding of the sense and purpose of data protection (which excludes a trivializing economization of data), nothing is gained in the sovereignty of those affected.

A further trivialisation of data protection consists in maintaining protection from advertising material for its cardinal problem. Here it is important to understand that in the context of "advertising", the prediction of behaviour and the targeted control of individuals on the basis of the evaluation of correspondingly collected data is now much more far-reaching. This must also be taken into account if a feeling of discomfort is formulated with US communications companies and secret services simply because their activities are not sufficiently transparent. It is about more than transparency, it is now also about subtle counterfeiting and manipulation of communications. The hacker risk is also seen as a major problem, according to which citizens must expect criminals to be able to access PCs at will. With each of these narratives, data protection is taken out of view or at least minimized. In addition, they suggest the idea that the individual concerned can only solve data protection on his own and for himself. In this respect, "self-protection" even appears to be the most promising risk management strategy, reserved (if at all) only for those IT experts who have mastered *privacy enhancing technologies (PET)*. No, it

is not the people who are to blame if organisations do not comply with data protection law.

After such false simplifications to the data protection problem, it is time to redefine the dimensions of the "risk concept" in the context of fundamental rights-oriented data protection. This provision must start with an effective implementation of the "*rights and freedoms of persons*", as the French formula calls it, which in German means "fundamental rights".

3 Risks in the context of GDPR

The EC 75 refers to the risks of poor data protection as "*physical, material or non-material harm*", "*where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;*" It also refers to cases where individuals are "*(...) deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles(...).*"

In one of the first German-language comments to the GDPR published by the Federal Ministry of the Interior Winfried Veil interprets the EC 75 under the problematic heading "risk-based approach". The "woodcut-like listing" does not convince him, among other things because the GDPR does not define the protected goods at any point against which the risk and/or the damages for rights and freedoms can be estimated (cf. Veil 2018: 721). It overlooks however that straight by the listing of possible damage the basic right reference gets lost. Instead of countering this problem, Veil expands the EC 75 list and adds further risks to it, which he tries to justify by saying that they are now "scientifically founded". As further risks Veil mentions: "increase of individual vulnerability through criminal acts", "shame and publicity damages", "selectivity damages" (undesired use of information in selection processes), "information permanence" (damages from unlimited storability of data), "decontextualisation", "information emergence", "information errors", "treatment of humans as objects", "heteronomy", "disappointment of confidentiality expectations" (Veil 2018: 724). The list of possible data protection risks in this concretion is thoroughly meritorious. But Veil obviously does not share the opinion that the risks mentioned by him are already completely captured by the principles in Article 5 GDPR! The protective property of the GDPR is, differently than

Veil claims, completely clearly proven: It concerns on the one hand the rights derivable from Article 5 GDPR that go back to Article 8 of the EU basic rights charter (GrCh). And it is on the other hand the resulting actual guarantees of freedom for persons who result from an effective conversion of these and further principles of the GDPR against the structural superiority of the organizations.

This interpretation of Article 5 requires a willingness to interpret the principles in terms of warranty and protection objectives, which must be methodically implemented in IT systems. Veil points out that in Article 5 the standard giver explicitly does not speak of protection goals (Veil 2018: 722). This reading is not convincing. Protection goals are now a methodically established instrument for identifying impairments, i.e. encroachments on fundamental rights and protection measures. In this respect, protection goals are a response to David Hume's insight in legal philosophy, according to which there is no should in being, and no should that can be directly generated from being. Exactly for this, for the mediation between being and should, mediating models are needed. Protective goals make both sides - technology and law - relevant to each other in a mutually gentle way and relateable to each other. The fact that at least the Federal Constitutional Court finds the concept of protection goals convincing was shown in the 2008 ruling on the confidentiality and integrity of IT systems (see BVerfG 2008).

A catalogue of implementation measures is available for each of the principles in Article 5 and the "Optimisation requirements for the protection targets" (Bock/Robrahn 2018), the impact intensity of which can be determined by the level of risk or protection requirement (cf. Hansen et al. 2015; SDM 2016). In the narrow sense, the risks for those affected lie in the fact that organisations do not observe the principles formulated in Article 5 GDPR or Article 8 GrCh. These principles and their implementation are it, against which each processing activity - for instance in the context of the data protection impact assessment in accordance with Article 35 or the Data Protection By Design in accordance with Article 25 - is to be planned, operated and not least also to be examined. The list of concrete expected damages in EC 75 provides additional support for this, but it is by no means sufficient to identify all essential data protection risks and to analyse, evaluate and appropriately process them with regard to the persons concerned.

Felix Bieker has presented a much more compelling approach to focusing privacy risks on the protection of rights and freedoms. Bieker first emphasizes the comparatively short passage of the EC 75, in which he explicitly mentions "immaterial damages" and "violation of the rights and freedoms of persons". In addition, he refers to EC 94, which once again expressly states "(...) that a risk includes not only a possible damage, but already the impairment of a fundamental right. For the fundamental right to data protection according to Art. 8 GrCh, this risk means that the impairment - already existing through any processing - is not reduced to the extent required for the protection of the natural person". (Bieker 2018: 29)

With regard to technical and organisational measures, this means that measures must be taken to reduce to the minimum possible the interference with and risks to the rights and freedoms which mere processing activities always and necessarily entail for personal data processing. It is not necessary to wait for a possible material (financial) or immaterial (damage to reputation) loss to occur in order to have identified a manifest data protection conflict.

4 Eight risk types

In a risk analysis, many commentators, and above all many data protection practitioners, refer exclusively to the risks specifically listed in EC 75 (typically: Schmitz 2018). Organizations can live very well with the resulting few protective measures to increase IT security. Veil, for example, reassures those responsible by saying that while "*(...) the extent to which risks arise from the specific type of data processing must be taken into account, it also reassures them of how they are limited again (...), for example, by technical and organisational measures, transparency measures or the possibility of asserting data subjects' rights. From the point of view of a responsible person, additional risk limiting measures can thus be a way to 'win' a balance of interests.*". (Veil 2018: 238, marginal 143)

These commentators misjudge the function of law in the handling of specific conflicts: law makes conflicts visible by giving them a communicable form.[4] However, the legal handling of a data protection conflict does not resolve the conflict; many data protection lawyers must keep this in mind. In order, for example, to promote environmental protection through appropriate environmental protection law, experts must also be consulted on the biological, chemical and physical properties of the environment, which can give the conflict between ecology and economy a communicatively accessible form that can then be dealt with politically, legally and scientifically. Similarly, experts for organisations, social structures and technical systems must be consulted for the implementation of data protection. This was also the case in the first phase of the development of data protection law in the 1970s (cf. Podlech et al. 1976). Since the lawyers took power in the data protection supervisory authorities, substantive analyses of central data protection conflicts have apparently been considered dispensable; data protection has been reduced to data protection law since the census ruling at the latest. Without considering the various dimensions of structural data protection conflicts, however, it is impossible

[4]The social reference, which the GDPR establishes in the EC 4 and 6, is remarkably weakly trained and obviously driven by the motive that data protectors are supposed to summon up understanding for the special needs of the data processors. One does not have to share the basic right compellingly the idea that data protection stands before new challenges through the "globalization" (EC 6). This is analytically misguided because it cannot be "globalisation", but international organisations that do not adhere to fundamental rights, among other things because their activities are not subject to effective data protection control.

to gain a benchmark for assessing the quality and impact of data protection activities (cf. Pohle 2018). The conflict to be dealt with by data protection does not consist in directly averting damage to individuals or in "preserving a snail-shell privacy" (Paul Müller), which never existed, but in the structural asymmetry of power between organisations as notorious risk takers and people as inferior risk takers. This asymmetry has been steadily intensified by the use of information and communication technology by organisations since the 1980s and has now become so entrenched that it appears that it can no longer be adequately dealt with by the current rule of law norms and controlling activities. Moreover, the separation of powers, the rule of law, markets and free discourses as modern sources of personal sovereignty and autonomy are no longer only threatened, they are in the process of dissolving.

There are incomparably more and different risks for persons who therefore address operational data protection and who the data protection supervisory authorities have to deal with both with regard to the direct protection of data subjects and to the protection of the social structures of modern societies.

- risk of legitimacy
- risk of legality
- risk of modelling
- risk of transparency
- risk of purpose limitation
- risk of IT security
- risk of data protection enforcement
- risk of political activities

If, however, no one demands that professional data protectors actually check that all risks are dealt with effectively, this will not happen.[5]

1. risk of legitimacy: Today it is quite possible for an organisation within the EU to carry out a personal processing activity which is not legitimate, i.e. which cannot be carried out in conformity with fundamental rights because its very purpose is unacceptable and does not take into account the subject quality of the data subjects. This objectification constitutes the core of any "automated decision" when machines seem to react intelligently to human activities. Automated individual case decisions are in this respect operational everyday life, naturally also with organizations, which have their company headquarters within the EU and are attainable in this respect from the GDPR. These forms of the data processing are to be found however in particular with the

[5] An intrinsic motivation is considered unprofessional among administrative employees. The employees of a data protection officer are not neutral administrative employees, nor are they judges who have to weigh up all the interests involved: They should decisively take sides for those affected.

throughindustrialized processing activities of American communication companies. If obviously illegitimate processing activities, in which personal data are regarded as peas, can be operated on a massive scale, this undermines the confidence of citizens in the legal system. At the same time, it is obvious that the state executive, in particular the security authorities, including their secret services, benefit from the unbridled actions of the companies whose data is readily accessed.i Why should a state want to end this win-win situation?[6]

2. risk of legality: Even if an organisation with a processing activity is in principle pursuing legitimate purposes, the legal basis which would remove the prohibition subject to authorisation under Article 6 GDPR (or Article 8 of the EU Charter of Fundamental Rights) for the purpose to be shown separately may be missing or insufficient. In the absence of a legal basis, this is initially to the detriment of the organisation, because it is precisely this absence that can be easily ascertained and sanctioned. Much more difficult it can be on the part of the data protection supervisory authorities or courts to judge whether a legal basis presented by the responsible person is sufficient for the justification of a processing activity. For the data subject, an existing, reliable legal basis means above all that the data controller has dealt with the data processing. This at least improves the chances that data processing is operated separately from other processing operations and that IT security measures have also been taken. If the purpose of a data processing is sufficiently narrow, the necessity of the data collection and possible "purpose extensions" in the enterprise can be proven in court. However the GDPR speaks for instance in art. 24 of processing purposes in the plural and facilitates legally justifiable purpose change in relation to the so far valid German data protection regulations.

3. risk of modelling: Even if data processing complies with data protection law, there is a risk that the practical implementation of the processing purpose will not reduce the intensity of the interference with fundamental rights by data protection measures to the absolutely necessary level. This is a frequently encountered constellation: data processing looks legally compliant at the conceptual level, but the operation is not, solely because the intensity of the encroachment on fundamental rights was not determined on the basis of a relevant attacker model or the intensity was underestimated. Therefore, two aspects have to be considered in the modelling: a) An attacker model has to

[6]Of course, the Federal Constitutional Court has long noticed this as well. Prof. Voßkuhle, the current President of the Federal Constitutional Court, already indicated in November 2011 that the BVerfG would deal with Facebook. "The President of the Constitutional Court warns against Facebook (...) He hinted that the Federal Constitutional Court could be forced to examine whether the Facebook offer is compatible with the right to informational self-determination. I don't want to anticipate the First Senate responsible for such questions. In any case, there are indications that the Federal Constitutional Court will be called upon in the coming years to redefine the significance and scope of fundamental rights in a world of digital networking.'". (RP-Online v. 6.11.2011, `http://www.rp-online.de/digitales/internet/Verfassungsgerichtspraesident-warnt-vor-facebook-aid-1.2542329`, retrieved: 21.01.2018).

be explicated: Who is an attacker with what motives and resources? b) What are the specific operational risks for the person affected?

a) From the point of view of data protection, the main attacker against persons or personal data is always the data processing organisation itself, but not, for example, "the hacker". The fact that the organisation which carries out the data processing has to be modelled as the main attacker forms the core of every fundamental-rights oriented risk determination and data protection analysis. On this basis, it is necessary to identify further structural attacker organisations and to estimate their access motives and resources to a processing activity. In concrete terms, the security authorities, service administration, providers of IT (infrastructure) services and critical infrastructures (such as energy providers), insurance companies and banks, tax offices, research institutes (especially psychological and social science), hospitals, doctors, lawyers, aggressive start-ups and advertising agencies must be taken into consideration. In the end, hackers and crackers, as well as inactive data protection officers or data protection supervisory authorities, are all risks that need to be taken into account.

zu b) The specific operational risks to be dealt with by protective measures can be found in the requirements of the GDPR. The principles from article 5 GDPR form a concretizing first starting point. Article 5 contains, partially unnecessarily verklausuliert, seven protection goals. If one negates these principles - a data processing does not become surely available, not integer, not trustworthy, not transparent, not narrowly purpose-determined, not changeable and operated only with the absolutely necessary data volumes - then concrete protective measures can be won from this approach. For example, the processing of personal data must be redundant, databases and communications must be encrypted, everything must be specified, documented and logged, it must be possible to effectively change and delete it, etc.. All this must be done with a view to protecting the persons concerned, not the organisations. The German data protection supervisory authorities, as well as the Federal Office for Information Security (BSI), recommend the use of the Standard Data Protection Model (SDM) to determine appropriate protective measures.[7]

Developing a risk analysis methodically along an attacker model that understands the organization as the attacker and focuses on protecting the affected persons, and that is not limited to risks and security deficiencies of the IT, is of course delicate. In many organisations, but also in many data protection supervisory authorities, there is a lack of willingness and experience to work out the data protection conflict so clearly. If the now demanded data protection impact assessment in Article 35 GDPR is carried out seriously and the data protection supervisory authorities do not let themselves be fobbed off with bad

[7]So far, application of the SDM in some supervisory authorities is not yet common practice, however, application of the SDM in some supervisory authorities is not yet common auditing and advisory practice (see SDM 2016).

simulations from it, it will become more difficult for organizations than so far to smear this conflict into the unrecognizable (see Forum Privatheit 2017).

4. risk of transparency: Even if an organisation conducts legitimate processing activities in a legally compliant manner and reduces the encroachment on fundamental rights to a minimum according to the state of the art, this activity is often not transparent in the sense of observable or even measurable in its real effects. Many characteristics of IT systems (hardware/software) and processes cannot be tested in practice, neither by those affected nor by the data protection supervisory authorities, nor by the responsible organisation (or its internal data protection officer). In most cases, this fails solely due to a lack of testing competence, as the complexity of information technology in particular has become very great. Establishing the transparency of data processing is not an end in itself (cf. Engeler 2018); transparency alone has a serving function: it is an essential prerequisite for controllability (for compiling all components relevant to the processing activity), verifiability (target/actual comparison of the activities of the components) and assessability (of the test results by legal experts) of processing activities with regard to whether those responsible have observed the principles in particular of Article 5 and other requirements of the GDPR and implemented them effectively. An organization that intends to comply with data protection requirements and installs the protective measures and testing tools must, however, reckon with the fact that even from these measures new risks emanate that cannot be recognized and mastered.

5. risk purpose limitation: Even if an organisation should process personal data in an orderly, legally compliant and transparent or verifiable manner, it is to be expected that the organisation will permanently undermine, expand or extend the purpose stated in the legal basis. This can happen deliberately, for example through the use of big data technologies, or spontaneously stimulated by special profit-taking opportunities that arise, through "slight unfairness" or through the creeping development of a careless culture of largely purpose-free data handling. Typically, rules are ignored and protective measures bypassed in safety-critical exceptional situations. The creeping undermining of the original processing purpose often occurs through new IT options and protective measures that are used to monitor employees, but whose use is not covered by the purpose. Many of the damages listed in the second half of EC 75 fall under the type of risk mentioned here.

6. risk of IT security: Of course, it is a risk for those affected if an organisation has not made an appropriate selection and dimensioning of protective measures for its operational data protection and IT security. It is these risks that the EC focuses particularly clearly and well on and which can be dealt with by the basic protection measures of the BSI. A further, often unnoticed risk in the context of IT security, however, is the necessity that the IT protection measures themselves must be configured in accordance with data protection law or operational data protection. This is because IT security measures must also be operated in compliance with fundamental rights. IT security measures

that do not comply with data protection generally intensify the encroachment on fundamental rights.

7. risk of data protection enforcement: Omitted or inadequate data protection controls represent a very high data protection risk in practice. This risk does not primarily result from the scandalously low staffing of the data protection supervisory authorities (cf. Schulzki-Haddouti 2015), but even more from their inadequate inspection quality.

Even if personal processing activities are audited by supervisory authorities, it is generally unclear what exactly and how data processing operations were audited. The transparency and integrity of most data protection audits by the supervisory authorities must be seriously questioned if no information about the audit standard and the audit method can be provided and if audit concepts, audit documents and audit records that go beyond the level of short reports to parliament cannot be presented.

The requirements that data protection supervisory authorities place on the processing activities of other organisations must be met by the supervisory authorities themselves in relation to their procedures - namely to monitor the processing activities of other organisations and to enforce the requirements of the GDPR (cf. Art. 57, para. 1 lit. a GDPR). Even if data protection examinations in the sense of the art. 5 GDPR are carried out sufficiently transparent, integer, purpose-oriented etc., for instance with recourse to the already mentioned standard data protection model, then negative test results remain on the part of the supervisory supervisory authorities often without consequences for the responsible data processor. In addition, negative audit results do not necessarily lead to improvements in processing activities, even if sanctions were imposed. In the case of multiple complaints in the activity report of a national representative, the already moderate sanction character is quickly lost if no further consequences are added.

But even if a data protection supervisory authority brings a data protection conflict with those responsible to court, courts often do not decide on the merits, but save themselves by complaining about formal errors. And even if a court is prepared to make a decision on the matter, the legal regulations often prove to be inadequate - which in turn suggests that the legislator has a continuing lack of interest in data protection.

8. risk of political activities: At present, no party can be identified in Germany that is able to analytically get to the bottom of the conflict to be dealt with by data protection and the resulting fundamental rights risks, apart from individuals, in particular the Greens. The same applies to NGOs or interest groups that quickly run out of air beyond obvious scandals (see Rost 2017). Those affected do not currently have a powerful advocate for their interests; the protective function of the data protection supervisory authorities is no longer worth mentioning. The predominant framing (cf. Wehling 2016) of political discourses on data protection dwarfs and trivialises the effective implementation of fundamental rights either, as shown above, to private matters or to a

risk of IT security, and takes the edge off data protection laws if, instead of insisting on their enforcement, well-intentioned ethical discourses are conducted, as the European data protection commissioner Butarrelli likes to practice. All of this benefits only the already overpowering organisations that continue to shape and control social communications. If data protection no longer meets with resonance from a party-political point of view - that was once different - then this could be an indicator that society is threatening to fall back into the pre-modern era in terms of social structure - in other words, into a time when a few organisations and individuals were still strictly hierarchically determining people's lives.

To put it succinctly, the thesis is: At present we can watch a modern, and thus sociologically soundly formulated, functionally differentiated society either regressing to a "stratified society" (Rost 2012) or "becoming old" (Lehmann 2015). The effective implementation of fundamental rights shows whether opportunities for modernization of functional differentiation are used.

5 Conclusion

The aggravation of the interpretation of risks of the GDPR on a risk-based-approch becomes itself the risk for a data protection interested in the effective conversion of basic rights for the interpretation of risks if the focus reduces to the concrete damages and control losses listed in recital 75 GDPR. At least the fundamental rights essential risks for persons then come into view if the conflict of the asymmetrical power relation between the organizations generating risks and persons constitutive for the data protection becomes the starting point of risk analyses. The GDPR gives, in particular with the principles of the data processing in Article 5 as well as the Articles 24, 25, 32 and 35 aiming at the effective conversion, a good framework for the determination and dimensioning of technical-organizational measures for the reduction of a multiplicity of data protection risks. Without a politically intended massive strengthening of the data protection supervision activities, which also lead to effective sanctions, the social relapse into the pre-modern age is, however, probable again, just because of the employment of particularly effective modern monitoring techniques.

6 References

- Bieker, Felix, 2018: Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell, in: Datenschutz und Datensicherheit (DuD), 2018, Nr. 1: 27-31.
- BSI 2017: Standard-200-3, Risikoanalyse auf der Basis von IT-Grundschutz, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html` (last retrieved: 20.01.2018).

- BVerfG 2008: Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 (=BVerfGE 120, 274 - 350), "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“.
- Engeler, Malte, 2018: Das überschätzte Kopplungsverbot. Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen; in: Zeitschrift für Datenschutz (ZD), Nr. 2: 55ff.
- Forum Privatheit, 2017: Whitepaper Datenschutz-Folgenabschätzung, 3. überarbeitete Auflage, https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-whi Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf (last retrieved: 20.01.2018).
- GDPR 2016: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Hansen, Marit / Jensen, Meiko / Rost, Martin, 2015: Protection Goals for Privacy Engineering, Proceedings for the International Workshop on Privacy Engineering, IWPE'15. (https://ieeexplore.ieee.org/document/7163220)
- Lehmann, Maren, 2015: Das »Altwerden funktionaler Differenzierung« und die »nächste Gesellschaft«, in: Soziale Systeme (Special Issue), Jg. 20, Nr. 2: 308-336.
- Podlech, Adalbert; Dierstein, Rüdiger; Fiedler, Herbert; Schulz, Arno (Hg.), 1976: Gesellschaftstheoretische Grundlage des Datenschutzes, Datenschutz und Datensicherung, Bachem-Verlag: 311-327.
- Pohle, Jörg, 2018: Datenschutz und Technikgestaltung (https://edoc.hu-berlin.de/bitstream/handle/18452/19886/dissertation_pohle_joerg.pdf).
- Robrahn, Rasmus; Bock, Kirsten, 2018: Schutzziele als Optimierungsgebote; in: Datenschutz und Datensicherheit (DuD), 2018, Nr. 1: 7-12.
- Rost, Martin, 2012: Zur Soziologie des Datenschutzes; in: Datenschutz und Datensicherheit (DuD), Nr. 37: 85-91. Rost, Martin, 2013: Eine kurze Geschichte des Prüfens, in: BSI (ed.), Informationssicherheit stärken – Vertrauen in die Zukunft schaffen, Secumedia-Verlag: 25-35.
- Rost, Martin, 2017: Bob, es ist Bob!, in: FifF-Kommunikation, Jg. 34, Nr. 4: 63-66.
- SDM 2016: The Standard Data Protection Model A concept for inspection and consultation on the basis of unified protection goals Version 1.0, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/