THE RISK-BASED-APPROACH IN DIGITAL DIMENSION AND "MOBILE SECTOR" (LIABILITIES AND AWARENESS OF A DATA CONTROLLER)

Manlio d'Agostino Panebianco
(BASC - Università Milano Bicocca)

Abstract: Digital Dimension, Cyber-security and Data processing have in common the risk management approach methodology: on the one hand, the evolution of ICT technology and, on the other hand, some legislation about financial and public services, recall the need to observe - in a critical and analytical way - the choice to concentrate many functions of daily life on a single mobile device. these considerations must, in fact, also be read in light of the legislation on the protection of personal data (GDPR, in particular), declined in relation to the principle of accountability, privacy-by-design and risk management methodologies.

Keywords: #risk-management #concentration #mobile-device #GDPR #privacy-by-design # cyber-security

1. Introduction

The considerations on which it is intended to dwell concern the awareness and responsibility of giving a correct technical guideline to those decision-makers in approaching to mobile device (and generally to digital dimension) and to risk management, and in particular recalling the need for a double perspective: not only technical (*i.e.*, of the provider), but also of the user.

Therefore, before getting into the merits of some delicate aspects which are the heart of this contribution, it is important and essential to make a brief - but necessary - premise.

The focus of this contribution is not to question (nor is it the author's will to do so) the freedom and natural technological evolution that increasingly leads to a *digitization* and *dematerialization* of activities. So, without any prejudice, it worth making some considerations on emerging issues, trying to find some technical, social and legal compliance approaches to better correctly face arising risks, that seems to be in several case under-evaluated.

First of all, to maintain an *anthropocentric approach*, in which the tools are at the service of the human person, and not the other way around. Then, to have a *holistic approach*[1], in which

1 M. d'Agostino Panebianco, *L'Holistic Complexity Approach*, in riv. *Statistica e Società*, 2019.

all aspects and factors are considered (grading and differentiating them, in the short-, medium- and long-term), especially when risks derive from these, which in particular nowadays seem under-estimated.

Therefore, the objective of this contribution is not to make a utopian critique of the orientation of some strategies already in place, but to stimulate a debate in the scientific community (both juridical and political, as well as technical) to improve the system, through dynamic/ongoing analysis of the situation.

Moreover.

Until a few years ago, when it was necessary to identify and address issues and problems related to information systems, we spoke generically of "*IT risk*". Today, international studies and surveys incorporate those "concerns" that highlight greater *complexity*, declining the different dimensions in which it can manifest itself.

In this sense, it is appropriate to recall the "*Global Risk Report*"[2] of the World Economic Forum from which it is clear that in addition to socio-economic, geopolitical and environmental factors mainly linked to the current context, they assume - and will continue to assume in the coming years - growing importance related to *data security*, *cyber-security*, *digitization*, the use of technology and innovation in general, both in terms of impact and probability of occurrence.

Methodologically, the choice made is to analyse and take as an example some *best practices* from different contexts and fields[3]: a multidisciplinary approach (that mainly reflects even the features of modern life) that allows to enhance knowledge, know-how and methods of approach, which have been successful previously, and which are known, in doctrine and literature.

The impact of new digital technologies on business models requires serious and careful reflection of a strategic nature on risk governance and opportunities associated with the phenomenon of "*digital transformation*" which, if not appropriately addressed, could generate serious (and sometimes, extreme) consequences[4].

In this context, a specific focus should be done on the issue of "*concentration*" – in the form of a broad aspect of *risk management* (i.e., referring to information, customers, suppliers, and/or a variety of different technologies, etc.)[5] - which does not in itself represent a novelty; however, it is necessary to highlight how in this global context in which Information and Communication Technologies (ICT) play a predominant role, it transversally influences all social, economic and legal effects.

2 The Global Risks Report explores some of the most severe risks we may face over the next decade, against a backdrop of rapid technological change, economic uncertainty, a warming planet and conflict. See World Economic Forum, The Global Risks Report 2024, January 2024, ISBN: 978-2-940631-64-3, available at https://www.weforum.org/publications/global-risks-report-2024/.

3 In several cases, the banking and financial field have been recalled, since that sector has a strong and detailed regulation, both at international and domestic level.

4 See Assirevi, *L'evoluzione della governance dei rischi di information technology - Modelli di governo da considerare per un efficace gestione dei rischi legati alla tecnologia*, Milan, May 2023, p.3

5 See A. Mantelero, *Big Data: I rischi della concentrazione del potere informativo digitale e gli strumenti di controllo,* in *Rivista Diritto dell'informazione e dell'informatica*, 2012, p.138

Therefore, in this context, it is necessary to reflect on the relative importance that must be given, in order to adjust the approach proactively, and not to suffer the expected negative effects, in the near future.

2. Information and data: the Risk Based Approach (Data-RBA).

In the "*digital dimension*"[6], it is relevant to refer particularly to *data processing*, in which it is adequate to notice that personal-data-processing is one of the main fields of application, but not the unique. In this context, it is proper to highlight the different meaning between *information* and *data*, and then of *personal data*.

According to Baškarada and Koronios[7] the concept of "*information*" can take on the meaning, referring to different authors, such as:

«*data which adds value to the understanding of a subject (Chaffey and Wood, 2005, p. 233)*»;

or even, «*data that have been shaped into a form that is meaningful and useful to human beings (Laudon and Laudon, 2006, p. 13)*»;

and more, «*an aggregation of data that makes decision making easier (Awad and Ghaziri, 2004, p. 36)*».

On the contrary, in principle, the "*data*" can be defined as a raw element, which requires further contextualization elements to take on a semantic value or concrete application. Still referring to Baškarada and Koronios[8], therefore, it could be defined as:

«*data has no meaning or value because it is without context and interpretation (Jessup and Valacich, 2003, Bocij et al., 2003, Groff and Jones, 2003)*»;

or even, «*data are discrete, objective facts or observations, which are unorganised and unprocessed, and do not convey any specific meaning (Awad and Ghaziri, 2004, Chaffey and Wood, 2005, Pearlson and Saunders, 2004, Bocij et al., 2003)*»;

and more, «*data items are an elementary and recorded description of things, events, activities and transactions (Laudon and Laudon, 2006, Turban et al., 2005, Boddy et al., 2005)*».

It is evident and clear that in the "*information society*", these two different elements have a complementary role and coexist, in a context of interchange and continuous interaction: furthermore, it is possible to observe on a daily basis both the growth in the volume of information and data, and the growing need to find ways of using it, with the creation of added value.

This circumstance led to the birth of the term "Big Data", i.e., the set of a mass - often not better quantifiable although significant - of information and data characterized by being "raw", therefore often not easily usable and usable due to an application and/or objective.

In this context, «*the evolution of Artificial Intelligence and Machine Learning techniques (which developed in parallel with that of ICT, with increasingly frequent interactions) has triggered a process*

6 Reference is made to the 3 dimensions (real, digital and virtual) on which each person, nowadays, expresses himself and relates in the social context. In this sense, see, Floridi identifies in the "infosphere" that space which *de facto* includes the real and digital dimensions, without no solution of continuity between the two: see L. Floridi, *Pensare l'infosfera, la filosofia come design concettuale*, Raffaello Cortina Ed., 2020.

7 S. Baškarada, A. Koronios, *Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*, Australasian Journal of Information Systems, Vol. 18, n.1, 2013, p. 7

8 S. Baškarada, A. Koronios, *Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension*, Australasian Journal of Information Systems, Vol. 18, n.1, 2013, p. 7

of "added value" use of Big-Data, giving life to the so-called "Smart Data"».[9] This latter one, can be classified as aggregate and refined data - deriving from processing and profiling processes - which allow "prompt" usability for predefined purposes, therefore with a clear added value, compared to Big Data.

In this context, it is appropriate to refer to GDPR[10] at article 4.1, where 'personal data' assumes the meaning of «*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*». As a matter of facts, the process of transforming "Big (personal) Data" into "Smart (personal) Data" could be traced back to the use of artificial intelligence techniques, which result in a *profiling process*, which according to GDPR, is «*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*»[11].

The above, recalls the need for Supranational Authorities to allow natural evolution (technological, social, economic), as well as the consequent free circulation of data and information, although balancing it with the ever-increasing need to protect the fundamental rights and freedoms of the human person (and so of *data subjects*). From which derive, on the one hand, the "*principle of accountability*"[12]; and, on the other, the risk-based approach.

It is worth remembering how some aspects (for example, related to *risk-management* and/or *security strategies*) dictated by the current and binding provisions on the matter (for example in the personal data protection, the GDPR), can have a positive scope and impact even in contexts of "non-personal-data", but which in any case have an equally significant added and strategic value (for example, related to company secrecy, intellectual property, patenting, etc.).

In this context, it is adequate to highlight the meaning of "risk", such referring to the possibility that the result (of any operation carried out by a person, natural or otherwise) is different from that expected *ex ante*: if we usually refer to risks with a negative meaning, it is equally true that there is the possibility[13] that the emerging result could also be positive[14].

On the other hand, in order to measure the possible different result, which may come out from an activity or occurrence, usually we refer to "*risk exposure*". In business field, risk exposure is often used to rank the probability of different types of variations (gain or losses), defining both the quantitative and qualitative nature, and to determining whether the quoted variations[15] are acceptable or unacceptable.

9 M. d'Agostino Panebianco, *Il "dato": bene immateriale con un proprio valore intrinseco*, in AmbienteDiritto.it, n.2, 2023, pp.177-178

10 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)

11 See GDPR, article 4.4

12 See GDPR, article 6.2

13 It happens often in the financial field.

14 In this circumstance, it is possible to classify it as "*speculative*".

15 Especially and mainly referring to losses.

The accountability can be described and declined as a «*dynamic and ongoing responsibility which, in a "top-down" process, actively involves all the other people - natural and otherwise - involved in various capacities in the processing processes, starting first and foremost with the Data Controller, and falling on everyone the lower and operational levels (from the DPO, to the various managers and "in charge", both internal and external)*»[16]. While, in this field, the risk-based approach is properly described in the "Guidelines 4/2019 on Article 25 Data Protection *by Design* and *by Default*"[17] of the European Data Protection Board (EDPB).

These guidelines aim to highlight the importance of Data-Controllers'[18] and Data-Processors'[19] responsibility in implementing the GDPR obligations when designing personal data processing operations, *inter alia*, giving examples and indications on how performing the risk analysis (in compliance with Articles 25); so each Controller - declining the principle of *accountability*, since the early stage of projecting, designing, and planning the data processing – can correctly identify the risks to the rights of data subjects, and consequently determining and implementing appropriate measures to effectively mitigate the identified risks, providing an effective guidance "on how to assess data protection risks and how to carry out a data protection risk assessment".

As a matter of facts, the EDPB highlights that «*a systematic and thorough evaluation of the processing is crucial when doing risk assessments*»[20].

The following considerations and reflections, regarding a specific risk, should be contextualized and interpreted in light of this framework[21].

2.1. A qualitative and quantitative approach for a risk-assessment

From a risk management perspective, it is proper to recall the so called "*theory of black swan*"[22] (which indeed is actually a metaphor) that refers to those events considered impossible to occur or, so rare that it was not possible to predict in advance (i.e., *unexpected event*).

It is proper to highlight that several times, events are recognizable as "*possible to occur*" (i.e. "*expected events*"), only after they have occurred, since analysts trace their characteristics

16 See M. d'Agostino Panebianco, *Vivere nella dimensione digitale*, Themis ed., 2022, II ed.

17 See European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, Adopted on 20 October 2020

18 According to GDPR article 4 (7) 'controller' means *the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*.

19 According to GDPR article 4 (8) 'processor' means *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller*.

20 European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, Version 2.0, Adopted on 20 October 2020, p.10

21 From the reading and declination of the GDPR and the aforementioned EDPB-Guidelines, it emerges more and more clearly that an evident and obvious error in approach can arise if this matter is considered to fall within the exclusive field of the legal sphere. On the contrary, the risk-based approach clearly highlights how the legal-compliance component is obviously important, but not exclusive: in this sense, the interactions between decisions of socio-economic impact, organizational and ICT aspects come into play, but also and above all the ability to achieve an adequate level of (a) management control and (b) compliance, both (b1) formal and above all (b2) substantial.

22 See N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, New York, 2010.

back to circumstances that were in fact known, although statistically "small" in quantitative terms.

As a matter of facts, «*Taleb refers to a black swan as an event with the following three attributes. Firstly, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Secondly, it carries an extreme impact. Thirdly, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable*»[23]. Therefore, it is possible to state that the classification of an event in a "black swan" is strongly related, alternatively or jointly:

a) to the lack of consideration of previous events with such characteristics;

b) to the presumption that the low probability cannot cause significant effects and/or impacts.

For this reason, in a Risk Assessment context[24], it is appropriate to combine and decline the "*Black Swan theory*" together with the "*Pareto principle*"[25], which represents a non-linear interaction: it asserts that for any given event, the 80% of effects is the result from 20% of all causes, meaning that a small cause, might have a significantly large(r) impact.

Therefore, when outlining a *scenario*, it is important to consider all the possible events to be represented, classifying them in two different ways: those that are well known (both in quantitative and qualitative terms), because they happened in the past; but equally those which, although they have a low probability of occurrence (quantitative aspect), can generate significant effects (qualitative aspect).

3. The risk of "*concentration*"

In literature - in particular in the banking field - the risk of *concentration* can be described as the one arising from the concentration to a single (a) counterparty, (b) sector or (c) country, and/or (d) deriving from those factors that have the same characteristics such as to (e) give rise to the same potential negative effect.

If, on the one hand, in doctrine this kind of risk is mainly taken in consideration and analysed in the banking/financial field, on the other hand, it is also true that there is a strong (and inseparably) relation between the evolution of the *financial market* and *Information and Communication Technologies* (so called, *Fintech*).

Therefore, the reasoning proposed in this contribution begins right from the original field of application (*i.e.*, the financial one), although its evolution will tend to consider this only as the "starting point", to deepen the issue of concentration risk in the field ICT, also considering other applications, both of a social, economic and relational nature.

Indeed, in risk management, it is true that risks might be assessed in different fields, through similar approaches, according to typical features.

---

23 T. Aven, *On the meaning of a black swan in a risk context*, in *Safety Science*, n.57, 2013, p.44

24 This has to be considered, both generally speaking in the field of Risk Management, and particularly when considering a Privacy Risk Assessment conduct by the Data Controller and/or Data Processor, as required by the accountability principle stated by GDPR, and as provided by EDPB, Supervisory Authorities and National Data Protection Authorities, in their guidelines.

25 This is also known as "Pareto's 80:20 Rule", taking its name from Vilfredo Pareto, one of the most important Italian economists who lived between XIX and XX Century. According to this rule, for many phenomena only 20% of the causes generates the 80% of the consequences. See P. Rogers, A. Salla, *ABCs of Z/OS System Programming*, IBM Redbooks, 2010, Vol. 11, p.169.

Many authors highlighted that the speed of technology evolution led to an underestimation of this kind of risk in many fields: for example, «*the case of Bitcoin shows that the risk of concentration must not be ignored*. […] *If one player controls the majority of computing power, it could start reversing new transactions, doublespend coins, and systematically destroy trust in the cryptocurrency*»[26]. This position, moreover, how this risk is strictly related not only to economic and financial aspects, but also – and probably mainly, at nowadays – to technologies ones, due to limited adopted solutions.

As a matter of facts, according to this affirmation, it is possible to introduce another ratio between the "*risk concentration*" and "*lack of substitutability*", analysing this issue from the perspective of systemic risks: «*risk is concentrated in a number of financial market infrastructures and systemically important financial institutions. But systemic risk can also arise from technical and IT concentration, including from operating systems and programs, cloud servers, and electronic network hubs. These "single points of failure" are especially important for the proper functioning of the financial system, as disruptions immediately affect large parts of the financial economy*»[27].

Moreover, in a *strategic*[28] approach, it is important to observe how modern companies increasingly resort to the form of outsourcing as a way to make costs variable, and above all to obtain a higher quality level of the individual services.

This usual and widespread managerial choice translates - in the *short* and *medium* term - into an optimization of resources; although in the *long* term, it could be transformed and manifested into a *strategic risk*, such as the loss of an important know-how, in less control in the execution of processes, but also (and perhaps, above all) in the concentration of core processes within a few companies.

The European Banking Authority (EBA)[29] in the final report on ICT and security risk management[30] states that ICT systems form the backbone of almost all banking processes and distribution channels, but they also support the automated controls environment on which core banking data are based, and the related technological innovation plays a crucial role, becoming more and more the source of competitive advantage.

As well, the EBA among the various risks that it identifies as essential to take into consideration, detects «*the increasing reliance on third parties for ICT services and products, often in the form of diverse packaged solutions and resulting in manifold dependencies and potential constraints and concentration risks*».

In this context, at least, two reflections are appropriate.

---

26 C. Stoll, L. Klaassen, U. Gallersdörfer, *The Carbon Footprint of Bitcoin*, MIT Center for Energy and Environmental Policy Research, 2018, p.11

27 L. Kaffenberger, E Kopp, *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*, Carnegie Endowment for International Peace, 2019, p.6

28 The word *Strategy* derives from ancient greek στρατηγός, *stratēgós*, a word composed of two terms: στρατός, *stratós* (*i.e.*, army); and ἄγω, *ágō*, (*i.e.*, to lead). Nowadays, according to Cambridge Dictionary, it can be defined as a long-range plan for achieving something or reaching a goal, or the skill of making such plans. In Business Management and or Project Management, (a) Strategy is usually represented as the element of long-term planning, with its own and related goals, and ways to achieve them: within it, both (b) Tactics (i.e., those medium terms' actions and decisions aimed at achieving specific goals, and accomplishing tasks to support a strategy); and (c) Operations (the third component that complements strategy and tactics) are defined.

29 The EBA is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.

30 See *EBA Guidelines on ICT and security risk management*, 2019, p.30

3.1. The risk of concentration: on mobile devices

First of all, on the risk of concentrating all the authorization and authentication systems of the modern citizen on a single mobile device: as a matter of facts, the most spread system is the "two-factor" or "multi-factor" authentication based on both (a) static login credentials[31] and (b) a dynamic one generated by the connection between a mobile device and a remote server.

The so called PSD2 regulations[32] brought, *inter alia*, a great innovation in terms of security in remote payment transactions, introducing the so-called Strong Customer Authentication (SCA)[33]: the operative and technological application of the security measures listed in the EU Regulations have been mainly introduced by installing each bank app in a smart-mobile device, starting from the assumption that the same is always with the legitimate account holder.

While on the one hand, it is acceptable that each person has his or her own mobile device (as if it were an extension of one's body), it is equally true that risks, often underestimated, derive from this.

The risk of concentration related to mobile device[34] is not theoretical, since (for example) one the most widespread and rapidly growing fraudulent techniques is the SIM swapping[35], a technique to get control of a phone number, that allows hackers to take advantage of two-factor authentication to gain access to your bank accounts, social media accounts, etc.

This circumstance, moreover, could configure not only the characteristics of the accident, but also those of the "personal data breach"[36], to be managed according and referring to GDPR guidelines.

It means that the exposure to concentration risk becomes the primary source of credential theft risk, significantly reducing (if not even nullifying) the cybersecurity measures adopted.

From a technical point of view, concentrating most[37] of the main daily activities on just *one device*, it should be considered that exposure to "*digital risks*"[38] increases significantly: therefore, during the assessment it should be appropriate to collect information and evaluate the potential scenarios deriving from their interactions[39].

---

31 *i.e.*, Id and password and/or PIN (personal identification number)

32 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

33 which is an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

34 For example, smartphones

35 also known as SIM-splitting, SIM-jacking, or SIM-hijacking

36 Referring to GDPR article 4(12) 'personal data breach' means *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*.

37 even, not to say, to concentrate "all of".

38 In the perimeter of "digital risks" are included several ones, such as Cybersecurity, Workforce, Cloud, Compliance, Third Party, Technology, Automation, Resiliency, Data Privacy, Social Engineering, etc.

39 It should be noted that, in a correct approach the risk assessment should be conducted using the Holistic Complexity methodology, and not only cause-effect one. For details on this matter, A. Capoluongo (eds), *Smart Cities tra Intelligenza Artificiale, Videosorveglianza e Data Protection, Edizioni Giuridiche Simone*, 2023, pp.157-168.

For example, referring to the "*Technology Risk*", the strategic nature of technology in any public and/or entrepreneurial activity has the possible interruption of services[40] as its weak point.

Recalling the "*Third party*[41]*risk*", it has to be highlighted that many entities (both public and private) adopted some spread social media as the main channel of communications, not considering that these are projected and introduced in the market for a different aim than being used as a public and "social blackboard".

One of the most important considerations should be taken into account - at least from a legal and risk management perspective - concerns the investigation and the definition of liabilities in case (for example) of a (temporary) crash-down of service/app that interrupt the continuity of a related public/private service.

For example, for those entities which chose[42] some social media to communicate with their own users, without considering the purpose of the tool itself: these, in fact, have no contractual "working" purpose, but only the creation, maintenance and exchange of relationships on a personal level, without any express guarantee (at least for the users) of *business continuity*.

Therefore, from a technical perspective, any under-evaluation of these sort of circumstances (beyond the fact that it is now a habit in daily practice) should be considered as a serious error of (under)evaluation when conducting the risk assessment. Then, it should be appropriate to exploit what the liabilities and who in responsible in such a case (*i.e.*, of a crash-down).

In this context, it is adequate to shortly recall even to "*resiliency*", which refers to the risk of a negative event following the adoption of a new technology and the difficulty of minimizing the damage caused. This type of risk has to do with the availability of business operations, and is mostly concerned with business continuity.

Resilience is defined, *inter alia*, as «*the ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management*»[43].

Therefore, when recalling and referring to "*resilience*", it is actually proper to adopt that methodology - in a framework of *business continuity* - that allows to operate effectively and efficiently, even in critical circumstances, based on the ability to plan *ex ante* an expected flexibility. As a matter of facts, in making a scenario, it is possible to "draw" some possible ranges of circumstances, but not to "predict" the exact sequence of different expected steps of a specific situation[44].

40 such as the potential unavailability of critical systems due to power failures, disruption of the backbone lines on which the data travel; electromagnetic disturbances, deriving from changed geophysical conditions, etc.

41 According to GDPR article 4(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data. In the field of data protection, according to GDPR, several times requires the formal appointment as External Data Processor, since this latter one processes personal *data* only on behalf of the Data Controller.

42 It is appropriate to recall the principle of the responsibility *in eligendo*.

43 Definition given by United Nation Office for Disaster Risk Reduction, UNDRR.

44 It is important to remember the meaning of risk, risk-exposure, and probability of occurrence.

So, "resilience" should be interpreted as the possible and different approaches allowed to manage the critical expected situation: a sort of "*margin for maneuver*".

In case of the absence of such expected flexibility, the Entity (*i.e.*, the Data Controller and/or Processor) is exposing itself to the "risk of resilience", *i.e.*, the "*ongoing inability*" to adapt and react positively to the critical circumstance it is facing.

In the context of ICT, a possible prevention and mitigation measure to the "*risk of resilience*", could be the implementation of an integrate business continuity and disaster recovery plan, assuring that alternative technological and organisational solutions are (in advance) analysed, planned and then performed within the emergency plan.

3.2. The right to an alternative

The second issue concerns[45] the constitutional legitimacy of obliging a citizen to have a mobile device, which requires at least an initial investment[46] and recurring costs[47].

This consideration should not be seen only from the point of view of an overall and global digitization, but rather from that of a shift (from the supplier to the customer) in management costs.

In several cases of digital divide and modern social exclusions forms[48], the lack of *substitutability* (and the consequent concentration risk) offers another perspective to be exploited, to better understand the perimeter of this issue.

An example can help to better understand this issue: in Italy, due to physical security measures in order to face and reduce the risk of robbery, bank's entrances are equipped with compasses with metal detectors. These cannot be used by people with certain types of physical disabilities, and so in order in order to prevent them from finding themselves in an "*embarrassment*" situation, banks have provided for a "*lateral*" access which allows them to access, after using an intercom connected to the staff inside the branch. This solution, *inter alia*, should be framed in the context of *security-by-design* and *privacy-by-design*[49], as a form of conjugation of the *principle of accountability*[50].

This simple (but effective) example describes the "*right to an alternative*", *i.e.*, a different way that allows not to violate other fundamental rights and freedoms.

In a dual perspective (both of risk management and legal protection of human rights) it therefore seems necessary that any "*by-design*" process should take into consideration the various alternatives, both to avoid a specific *risk of concentration*[51], and to guarantee the correct exercise of individual freedoms and fundamental rights.

3.3. A dual approach

45 at least theoretically.
46 For example, purchase of the device
47 *i.e.*, subscription to the telephone network, electricity, etc.
48 Related to and deriving from poverty, difficulties to access to digital devices, smart cities, low level of education, etc.
49 *i.e.*, integration during its own lifecycle, from the early design stages to implementation, usage and ending of the processes.
50 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), Article 5.2
51 which moreover would be a source of further risks.

Probably, in the light of the quoted issues and the evolving dynamic situation, a new more complex approach is required: considering that there is a convergence and coexistence of two different fields (the legal and the risk management one), the "*risk assessment*" should be influenced and characterized by the "*balancing of interests*".

According to Blaauw-Wolff, this latter one can assume different meanings, depending on the circumstances. Mainly the process of balancing the interest can be referred to the «*weighing up of competing basic constitutional values. It implies that one interest or right takes precedence over another and that the preference afforded that particular interest or right renders the other one as subordinate to the one taking priority. This approach threatens the inner cohesion of the Constitution's founding principles, and does not promote equal respect for all the fundamental rights*»[52]. As well, «*it might refer to the approach of attaining a harmonious concretisation or practical concordance of competing provisions*»[53].

Moreover, it should be added that some authors argue that – in the perimeter of what can be defined "sociological jurisprudence"- there is an important (and sometimes, it is prevalent) judicial "balancing" approach that became what «*one scholar calls it one of the "most distinctive features of modern judicial practice"* »[54].

On the other hand, the *risk assessment* is a process of identification of potential adverse effects resulting from exposure of different kinds hazards: the risks involved may be expressed in quantitative or in qualitative terms: «*the fact that exposure to many potential hazards can occur simultaneously and in varying degrees dictates that the risk assessment process is complex*»[55].

4. Conclusions and follow-up

The evaluation of the "*risk of concentration*" (especially, in *mobile* sector) should be lead taking in consideration both the most traditional aspects (such as economics ones), but also those related to an exposure to a negative impact deriving from an expected reduction of fundamental freedoms and/or rights.

As a matter of facts, it could become very dangerous in not having a supranational political and ethical approach, letting both economic interests and ITC evolution lead this process, without a clear framework.

Indeed, if the market, *lato sensu*, reaches a very widespread level of pervasiveness in the distribution of such applications, it would be very complex and difficult (if not downright, impossible) to subsequently be able to take a step back (in the case of conscious, but belated, understanding of this issue).

52 H. Mostert, *Liberty, Social Responsability and Fairness in the context of Constitutional property protection and regulation*, in H. Botha, A. van der Walt, J. van der Walt (eds), *Rights and Democracy in a transformative Constitution*, Sun Press, 2003 p. 153

53 ibidem

54 G.F. Intoccia, *Reassessing Judicial Capacity to Resolve Complex Questions of Social Policy*, in *Journal of Legal Studies*, United States Air Force Academy, Department of Law, vol.11, 2001, p.141

55 Risk Assessment, United States. Environmental Protection Agency. Office of International Activities, 1992, p.3