B. Conceptual definitions as a link for regulation

This chapter clarifies the conceptual definitions that provide a link for the regulation of innovation. While the first sub-chapter refers to economic theories defining the terms "innovation" and "entrepreneurship", the second sub-chapter draws the attention to the other side, i.e. data protection law as a regulation of risks caused by innovation. This sub-chapter illustrates the discussion on various protection instruments for different types of threats, such as prevention and precaution or dangers and risks. This leads to the last sub-chapter treating the question of what is actually threatened. The clarification of the interplay between "context" and "purpose" provides a first understanding of the meaning and extent of the principle of purpose limitation.

I. Innovation and entrepreneurship

If the regulator refers, at least implicitly, to entrepreneurial innovation, it permits one to tie definitions that have been developed by other research disciplines.[80] Indeed, in other disciplines, there is not a common definition of "innovation" or "entrepreneurship". Scholars consider that innovation and entrepreneurship are phenomena that can and should be analyzed from various, interdisciplinary perspectives. This might be the reason for the lack of common definitions.[81] However, as one of the first economists, Schumpeter recognized, coming from an evolutionary understanding of private markets, innovation as an essential force for societal change. In his work *Capitalism, Socialism & Democracy*, he disagreed with the common view on price competition as the main driver of economy and determined, instead, "the new consumers' goods, the new methods of production or transportation, the new markets, the new forms of industrial organization

80 See Hoffmann-Riem, Openness toward Innovation and Responsibility for Innovation by means of Law, p. 257.

81 See regarding the first term at Fagerberg, Innovation: A Guide to the Literature, p. 1, and regarding the second term at Fueglistaller et al., Entrepreneurship – Basics, p. 6.

that capitalist enterprise creates" as the fundamental impulse "that sets and keeps the capitalist engine in motion".[82] From this perspective, the "function of entrepreneurs is to reform or revolutionize the pattern by exploiting an invention or, more generally, an untried technological possibility for producing a new commodity or producing an old one in a new way (…) and so on."[83]

Hence, Schumpeter differentiated between inventions, i.e. the first realization of a solution for a problem, and the innovation bringing an invention to the market.[84] This differentiation is, until today, widely recognized. Today's economists are focusing, in essence, on four types of innovations: First, product and service innovations; second, process innovations; third, business model innovations; and fourth, social innovations which often refer to new forms of communication or cooperation being mostly considered, actually, either as the basis for the before-mentioned types of innovations or as their result.[85] Further categories classify innovations pursuant to their impact on current production processes or market structures. This perspective differentiates between: on the one hand, "incremental" or "marginal" innovations describing continuous improvements of one or more innovation types listed previously; and on the other hand, "radical" innovations or "technological revolutions" referring to the introduction of a new technology or cluster of technologies which did not exist before in society.[86] Keeping this in mind, it is common ground today that data provides, more and more, the basis for many, if not once most, of these types or categories of innovation.[87]

82 See Schumpeter, Capitalism, Socialism & Democracy, pp. 82 and 83.
83 See Schumpeter, ibid., p. 132.
84 See Fagerberg, ibid., p. 5; Fueglistaller et al., Entrepreneurship – Innovation and Entrepreneurship, p. 98.
85 See Fueglistaller, ibid., pp. 99 and 100; cf. also Neveling et al., Economic and Sociological Approaches of Innovation Research, pp. 369 and 370, as well as Fagerberg, ibid., pp. 8 and 9.
86 See Fagerberg, ibid., p. 9 referring to Schumpeter.
87 See, instead of many, at Mayer-Schönberger and Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, in particular at pp. 6 to 35 and 322 to 336.

1. Process of innovative entrepreneurship

Entrepreneurship research poses, in particular, the question of how entrepreneurs create such innovation.[88] After researchers had initially focused on the personality of the entrepreneur per se, Drucker stressed, in his influential article *The Discipline of Innovation*, that it is less the personality per se that constitutes entrepreneurship than the entrepreneurial activity.[89] Over time, several economics had elaborated on models describing the entrepreneurial process as the overarching unit of analysis encompassing entrepreneurial phenomena such as activity, novelty, and change.[90] In order to extract a common model being both generic, i.e. describing the common patterns of all different kinds of entrepreneurial processes, as well as distinct, i.e. differentiating entrepreneurial from non-entrepreneurial processes, Moroz and Hindle analyzed more than 32 of existent models. They came to the result, however, that the models analyzed were too fragmented in order to achieve the initial aim of building a common model being both generic and distinct.[91] Despite this fragmentation, or rather because of it, three aspects shall be explained in more detail because they may serve as reference points for answering the question of how legal regulation instruments function with respect to the logics of entrepreneurs creating innovation.

a) Key Elements for the entrepreneurial process

The first aspect being of interest for this doctoral thesis refers to key elements which are decisive for entrepreneurship. Gartner elaborated on several of these key elements, who conducted, in the 1980's, a study with academics, practitioners and politicians related to the entrepreneurial field in order to gain a more comprehensive understanding about what kind of ac-

88 See Drucker, The Discipline of Innovation, p. 3.
89 See Drucker, The Discipline of Innovation, p. 3.
90 See Moroz and Hindle, Entreneurship as a Process: Toward Harmonizing Multiple Perspectives.
91 See Moroz and Hindle, Entreneurship as a Process: Toward Harmonizing Multiple Perspectives, p. 781.

tivity or situation is considered as entrepreneurial.[92] Pursuant to this model, entrepreneurs locate business opportunities, accumulate resources, and build organizations in order to produce and market products or services, while constantly responding to their environment.[93] Moroz and Hindle stress that this model does not actually describe a behavior being distinct to others, such as pure managerial activities. However, they also point to the implicit distinctness of this model describing the entrepreneur as being "involved in a multidimensional process of organizational emergence that is focused upon the creation of a new venture that is independent, profit oriented, and driven by individual expertise. The newness attached to this process is linked to products, processes, markets, or technologies where the firm is considered a new entrant or supplier to a market."[94]

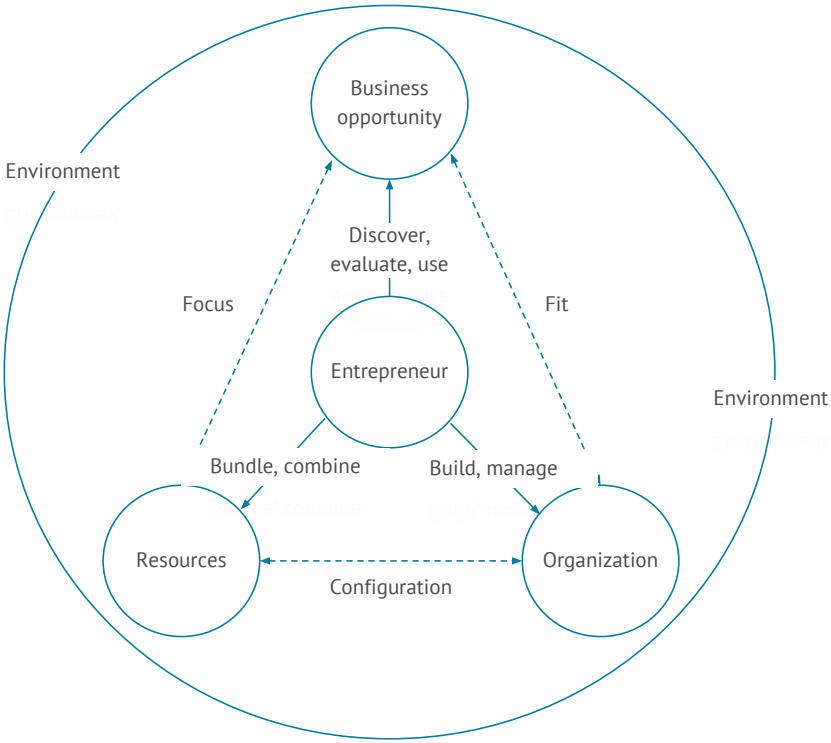
Fueglistaller proposes a very similar process model determined by the following five key elements: The entrepreneur, a business opportunity, sufficient resources, a form of organization, and a supportive environment.[95]

92 See Gartner, What are we talking about when we talk about entrepreneurship?, as well as, A Conceptual Framework for Describing the Phenomenon of New Venture Creation.

93 See Gartner, A Conceptual Framework for Describing the Phenomenon of New Venture Creation, p. 702.

94 See Moroz and Hindle, ibid., p. 800.

95 See Fueglistaller et al., Entrepreneurship – Basics, p. 7.



Graphic: Key Elements for Entrepreneurial Process[96]

Consequently, the entrepreneur constitutes the core of an enterprise discovering or creating business opportunities, evaluating and using them. In such an emergent process, the individual capacities, capabilities, and attitudes play a decisive role. The entrepreneur's cognitive capacities influence the identification or creation of business opportunities; the evaluation of the opportunity depends, on the one hand, on the characteristics of the opportunity and, on the other hand, on the individual attitude such as toward risks; and the use of the opportunities depends on the abilities of how to practically organize the process as a whole.[97]

96 Following Fueglistaller et al., ibid., p. 8.
97 See Fueglistaller et al., ibid., pp. 7 to 14.

b) Business Opportunities: Discovery and creation

The second aspect focuses on how entrepreneurs identify or create business opportunities. Economics usually consider the existence of a "business opportunity" if "there is an opportunity to introduce a new product, new service, or new method and to sell it for a higher price than its production costs".[98] They also agree on the assumption that such an opportunity arises "whenever competitive imperfections in an industry or market exist".[99] However, economics argue about from where these market imperfections come: Does an entrepreneur discover or create these market imperfections and, as a consequence, the business opportunity?

There are two main theories seeking to answer this question, the Discovery- and Creation Theory. Tying into teleological theories of human action, both theories aim to explain the relationship between entrepreneurial action and the ability to produce innovation.[100] Alvarez and Barney summarize the essential differences between both theories as:[101]

	Discovery Theory	**Creation Theory**
Nature of Business Opportunities/Market Imperfections	Caused by exogenous shocks to pre-existing industries or markets	Caused by endogenous actions of individuals to produce new products or services
Nature of Entrepreneurs	Entrepreneurs are different than non-entrepreneurs in some critical and enduring ways	Entrepreneurs may be the same or different than non-entrepreneurs; any differences, ex ante, may be magnified by entrepreneurial actions
Nature of Decision Making	Those who are aware of and seek to exploit opportunities operate under conditions of risk	Those creating opportunities act under conditions of uncertainty

Table: Differentiating aspects of Discovery and Creation Theories[102]

98 See Fueglistaller et al., ibid., p. 10: "Im Allgemeinen spricht man von einer unternehmerischen Gelegenheit, wenn sich die Möglichkeit bietet, ein neues Produkt, eine neue Dienstleistung oder eine neue Methode einzuführen und zu einem höheren Preis als die Produktionskosten zu verkaufen."

99 See Alvarez and Barney, Discovery and Creation: Alternative Theories of Entrepreneurial Action, p. 6.

100 See Alvarez and Barney, ibid., p. 2 to 4.

101 See Alvarez and Barney, ibid., pp. 2 and 6.

102 Following Alvarez and Barney, ibid., p. 6.

The last category, i.e. the nature of decision making, clarifies the interplay of both theories. Alvarez and Barney differentiate, pursuant to the possibility and probability of outcomes, between the terms "certainty", "risk", "ambiguity", and "uncertainty": While the term "certainty" refers to situations were a certain outcome is sure, entrepreneurs act under conditions of "risk" if they know (or are able to know) which outcome is possible and under which degree of probability; in contrast, an outcome is "ambiguous" if an entrepreneur has sufficient information (or are at least is able to retrieve it) in order to foresee that an outcome is possible but does not have enough information that he or she would able to determine its probable or likely outcome. Finally, an entrepreneur acts under "uncertainty" if he or she does not even know that outcome is possible). This differentiation allows one to clarify the knowledge-related pre-conditions of each theory: While the Discovery Theory assumes that entrepreneurs are able, principally, "to predict both the range of possible outcomes associated with producing new products or services, as well as the probability that these different outcomes will occur"[103], the Creation Theory "assumes that the end of an emergent process cannot be known from the beginning."[104] In such an uncertain situation, entrepreneurs are, hence not able to calculate, based on a risk-calculation methodology the opportunity costs related to their actions. As a consequence, the Creation Theory instead proposes focusing on the losses an entrepreneur can accept if his or her actions do not lead to a successful outcome.[105]

Alvarez and Barney draw from these assumptions the following implications: "Discovery Theory suggests that entrepreneurs maximize their probability of success by (1) carefully collecting and analyzing information about opportunities to calculate their return and possible opportunity costs, (2) developing a rigorous business plan that describes the opportunities they are going to pursue, and (3) obtaining capital to execute these plans from outside sources. Creation Theory suggests that entrepreneurs maximize their probability of success by (1) engaging in iterative, incremental, and inductive decision making, (2) developing very flexible and constantly adjusting business plans, and (3) obtaining capital from friends and family—people who are willing to bet on them and not on the oppor-

103 See Alvarez and Barney, ibid., p. 13.
104 See Alvarez and Barney, ibid., p. 20.
105 See Alvarez and Barney, ibid., pp. 20 and 21.

tunities they may or may not exploit."[106] Alvarez and Barney stress that the Creation Theory may also solve problems that appear to arise in other economic research fields, such as in strategic management theories. For example, these theories could not explain, so far, the reason for the empirical finding that entrepreneurs generate competitive advantages by using "valuable, rare, and costly to imitate resources".[107] The Creation Theory can explain such phenomena, arguing that the path dependency of a process emerged under uncertainty "is likely to generate resources that, from the point of view of potential competitors, are intractable (…) and causally ambiguous (…)."[108]

The differences between both theories do not mean that they must be considered, practically, as exclusive to each other. Instead, the conditions under which entrepreneurs act rather clarify which theory is more appropriate for predicting successful entrepreneurial behavior in specific situations. In situations where the entrepreneur has sufficient knowledge or, at least, is able to retrieve it in order to determine the risks, his or her actions lead more likely to successful innovation if they are consistent with the Discovery Theory; in contrast, if the entrepreneur acts under uncertainty, thus, is not even able to foresee that a specific outcome is possible, he or she will more likely be successful when acting consistent with Creation Theory.[109] Indeed, Alvarez and Barney also stress for cases in between: First, ambiguous situations where an entrepreneur has enough information to foresee that an outcome is possible, but not its probability; in these cases their predictions are less clear.[110] Second, there are also situations where the advantage of one process methodology toward the other one may change over time if entrepreneurs are moving from "risky" to "uncertain" situations, and vice versa.[111] In any case, both theories provide illustrative examples of how economics conceptualize the action-related logics of entrepreneurs and which role legal regulation may play with respect to the knowledge base for their activities.

106 See Alvarez and Barney, ibid., p. 32.
107 See Alvarez and Barney, ibid., p. 36.
108 See Alvarez and Barney, ibid., pp. 36 and 37.
109 See Alvarez and Barney, ibid., pp. 33 and 34.
110 See Alvarez and Barney, ibid., p. 35.
111 See Alvarez and Barney, ibid., p. 34.

c) Strategic management: Causation and effectuation

This leads to the third aspect being of interest for this thesis. Economics discuss two approaches describing in more detail the different logics of how entrepreneurs may decide and act in specific situations named "causation" and "effectuation". Sarasvathy describes these two approaches as: "Causation processes take a particular effect as given and focus on selecting between means to create that effect. Effectuation processes take a set of means as given and focus on selecting between possible effects that can be created with that set of means."[112] Sarasvathy exemplifies the implications of this approach as:

	Causation Processes	**Effectuation Processes**
Givens	Effect is given	Only some means or tools are given
Decision-making selection criteria	Help choose between means to achieve the given effect Selection criteria based on expected return Effect dependent: Choice of means is driven by characteristics of the effect the decision maker wants to create and his or her knowledge of possible means	Help choose between possible effects that can be created with given means Selection criteria based on affordable loss or acceptable risk Actor dependent: Given specific means, choice of effect is driven by characteristics of the actor and his or her ability to discover and use contingencies
Competencies employed	Excellent at exploiting knowledge	Excellent at exploiting contingencies
Context of relevance	More ubiquitous in nature **More useful in static, linear, and independent environments**	More ubiquitous in human action **Explicit *assumption* of dynamic, nonlinear and ecological environments**
Nature of unknowns	Focus on the predictable aspects of an uncertain future	Focus on the controllable aspects of an unpredictable future
Underlying logic	To the extent we can predict future, we can control it	To the extent we can control future, we do not need to predict it
Outcomes	Market share in existent markets through competitive strategies	New markets created through alliances and other cooperative strategies

Table: Differentiating Aspects of Causation and Effectuation Processes (words in bold and/or italic highlighted by the author)[113]

112 See Sarasvathy, Causation and Effectuation, p. 245.
113 Following Sarasvathy, ibid., p. 251.

Fueglistaller et al. refer to both approaches in order to illustrate the process of strategic management. They define the term "strategy" as the "systematic planning of all business activities and processes in order to pursue long-term competitive advantages."[114] The classic strategic management process is usually categorized along four phases: Analysis, development of strategic goals, strategic execution, and control.[115] In contrast to such a linear-causal approach, the effectuation approach focuses on the means available in a specific situation and the iterative-nonlinear development of the strategic aims. The effectuation approach thus, fits well situations defined by many unknown factors in which, for example, startups mainly operate.[116]

d) Entrepreneurial contexts: The Law as one influencing factor in innovation processes amongst others

Focusing on specific situations and the means actually available for an entrepreneur, the context plays a more important role. Welters highlights the importance that specific historical, institutional, societal and social contexts can have in determining the resources, as well opportunities and boundaries for entrepreneurial activities. From this perspective, the legal regulatory framework is, as an example of formal institutions, one impact factor for "entrepreneurship as taking place in (further) intertwined social, societal, and geographical contexts, which can change over time and all of them which can be perceived as an asset or a liability by entrepreneurs" (word in brackets added by the author).[117] Welters also stresses the recursivity of links between these contexts during the entrepreneurial process.[118] Innovation produced by entrepreneurs hence, is not the result of a one-dimensional and linear process, but of a multi-factor-based non-linear process.[119] Fagerberg highlights this interdependency as an essential rea-

---

114 See Müller et al., Entrepreneurship – Strategy and business model, p. 138: "Strategie: Die planvolle Ausrichtung sämtlicher Unternehmensaktivitäten und -prozesse zur Erzielung langfristig wirkender Wettbewerbsvorteile."
115 See Müller et al., ibid., p. 143.
116 See Müller et al., ibid., p. 147 to 150.
117 See Welter, Contextualizing Entrepreneurship, pp. 172 and 176.
118 See Welter, ibid., pp. 177.
119 See Neveling et al., ibid., pp. 371 and 372 with references to J. S. Metcalfe, Impulse and Diffusion in the Study of Technical Change, Futures 13 (1981), p. 347,

son for why many inventions take time turning, if at all, into an innovation as: "There may not be sufficient need (yet!) or it may be impossible to produce and/or market because some vital inputs or complementary factors are not (yet!) available."[120] Mayer-Schönberger concludes from this that many current laws suffer from a conceptual flaw because they would imply, in his opinion, a linear model of innovation processes. Taking the multi-dimensional and non-linear model seriously, the legislator should give up its reactive approach and understand itself, instead, as proactive actor directly creating – equally beside the other mechanisms (be they technical, social, cultural etc.) – business opportunities, and not only facilitating them.[121]

2. Regulation of innovative entrepreneurship

The preceding illustration of Entrepreneurship theories provides several links in order to answer the question of how innovation may be regulated through the law. First, considering entrepreneurs as the main driver of innovation (in which organizational form ever this occurs)[122] they appear to be appropriate addressees of laws aiming to regulate such innovation. Second, the action-oriented approach of entrepreneurship theories, in particular, the Discovery and Creation Theory corresponds to the regulatory approach applied in this thesis, which focuses, equally, on action.[123] Third, entrepreneurship models describing the entrepreneurial process correspond with the observation made in practice, as well as in regulation theory, that innovation often, if not mainly, occurs in highly dynamic non-linear processes, and not in causal-linear ways.[124] There are indeed causal-linear innovation processes, such as in research science; however, academics stress that most innovations do not occur in research settings but instead is driven by the experience of users and, thus, in more non-linear

---

as well as K. J. Schmidt-Tiedemann, A New Model of the Innovation Process 25 (1982), pp. 18 ff.

120 See Fagerberg, ibid., pp. 5 and 6.

121 See Mayer-Schönberger, The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship, pp. 180 to 183.

122 See Fueglistaller et al., Entrepreneurship – Basics, pp. 12 and 13.

123 See above under point A. II. Research questions and approach.

124 Cf. above under point A. I. 4. Practical examples referring to two typical scenarios, and A. II. Research questions and approach.

environments.[125] Finally, the context-oriented view of entrepreneurship research corresponds with the self-understanding of the regulatory approach considering the law as just one mechanism beside further ones, such as informal norms or geographical conditions.[126] Even if there is neither a common understanding of innovation or entrepreneurship research, in general, nor a holistic theory of entrepreneurial processes and its contextualization, in particular, the preceding aspects make it suitable as a conceptual model of reality for doing research on the effects of legal regulation instruments on processes of innovation.[127] The following paragraphs shall shed further light on the various effects of regulation on "innovative entrepreneurship" discussed in entrepreneurship as well as legal literature.

a) Do laws simply shift societal costs either protecting against or being open to innovation?

The legislator may shape laws conflicting with the non-linearity of innovation processes in order to protect individuals concerned. The principle of purpose limitation could be considered as an example for such a law, at least so long as it requires from the controller to exactly specify the intended use of personal data and then strictly limit the later use to this initial specification. Such an understanding of the principle of purpose limitation principally conflicts with the openness of innovation processes because it does not allow controllers to use the data for purposes other than for those that the controller could foresee when the data is collected. Mayer-Schönberger describes such a law as simply shifting costs between different groups in society. He gives an example of labor law in order to illustrate his opinion: The legislator can structure labor law in such a way, allowing entrepreneurs to easily hire and fire employees. On the one hand, this would enable entrepreneurs to save costs, i.e. constantly adapt expenses for human resources to the actual need at low transaction costs. On the other hand, either the employee concerned has to bear the costs for finding new employment (or other ways of financing his or her living expenses) or

125 See Fagerberg, ibid., Box 1.3 "What innovation is not: the linear model", p. 11.
126 Cf. above under point A. II. Research questions and approach.
127 See again Fagerberg, ibid., p. 1; Fueglistaller et al., ibid., p. 6; Moroz and Hindle, ibid., p. 781; Welter, ibid., p. 177.

the state for supporting the unemployed.[128] In light of this, the principle of purpose limitation as described before may be considered as simply shifting costs from the individual concerned to the controller referring to an assumption as: If the later use of personal data is limited to the originally specified purpose, the individual (or the social welfare state) may suffer less harm and though have less costs; the controller bears these costs, in turn, being limited in its innovation process.

b) Principles between openness toward innovation and legal uncertainty

In contrast, the legislator might also choose another way and decrease costs overall. Instead of shaping a law that only shifts costs from one group in society to another, the legislator might "also influence the probability of incurring a cost even when holding expected values (and thus costs for taxpayers) constant, thus prompting more people to engage in entrepreneurial activity".[129] In the first instance, principles may be considered as such a regulation instrument. As illustrated in the introduction, the legislator does not often have sufficient knowledge for determining precisely the circumstances of an entrepreneurial process and its impact on society. Therefore, the legislator can choose to establish principles, which leaves private companies more room in finding the best solutions themselves in order to meet the regulatory aim. Indeed, this form of regulation decreases legal certainty because the companies are not able to state whether or not they actually meet the regulator's exact expectations.[130] So far, at least, from this perspective, the principle of purpose limitation does not simply shift costs from the individuals to the controllers. Instead, it gives controllers room to find the best solution to apply the principle of purpose limitation and, thus, different ways of avoiding costs, not only for themselves, but also for the individuals concerned. This approach assumes that it is possible, in principle, for the controller to use, for example, personal data in a very broad way, or even for another purpose than initially specified, so that the way the data is being used does not harm the individual, and thus, does not lead in an increase in costs for the individual or so-

128 See Mayer-Schönberger, ibid., with further examples on pp. 175 ff.
129 See Mayer-Schönberger, ibid., p. 180, see also pp. 176/177.
130 Cf. again Raab and De Hert, ibid., p. 278; Eifert, ibid., cip. 25 and 26; Franzius, ibid., cip. 7, 17, 81 to 103;.

ciety. If this assumption turned out to be correct, i.e. no costs for the individual or society, the subsequent question is: what impact the decrease of legal certainty has on entrepreneurial activity.

aa) Legal (un)certainty as a factor that mediates the regulatory burden

In order to answer this question, two empirical studies shall be highlighted. First, the study conducted by Hartog et al. examined the impact of the regulatory burden and rule of law on entrepreneurial activity. Their results confirmed previous works "suggesting that social security entitlements, taxes, and employment protection legislation are negatively associated with (different forms of) entrepreneurial activity."[131] This result corresponds to Mayer-Schönberger's understanding of the type of regulation that shifts costs from one group in society to another. However, their study additionally came to the (seemingly) counter-intuitive result that countries with stronger rule of law had lower entrepreneurial activities. The authors considered this result as counter-intuitive because they assumed that a strong rule of law would not only hinder entrepreneurial activity, but would also help entrepreneurs, for example when they want to enforce their own contracts that they have concluded with third parties.[132] Hartog et al. considered that a possible reason for this result was that because, in developed countries, primarily large enterprises profit from the benefits of a strong rule of law.[133] The second study, which was conducted by Levie and Autio, proposes a more detailed explanation for this phenomenon: "Entrepreneurial and new ventures face disproportionately high compliance costs, because their small initial size makes it costly for them to maintain compliance functions internally. For industry incumbents, whose large size permits a greater degree of internal specialisation and the maintenance of a larger administrative function in absolute terms, compliance costs are less significant."[134] If one were to pre-suppose that there is a causal relationship, these considerations lead to the result that higher legal

131 See Hartog et al., Institutions and Entrepreneurship: The Role of the Rule of Law, p. 3.
132 See Hartog et al., ibid., p. 8.
133 See Hartog et al., ibid., p. 3.
134 See Levie and Autio, Regulatory Burden, Rule of Law, and Entry of Strategic Entrepreneurs: An International Panel Study, p. 1411.

certainty hinders innovative entrepreneurs, rather than enabling them to pursue their activity. At least this is the case, so long as the entrepreneur's organizational structure remains so small, that the bearing of compliance costs still is disproportionate.

In this study, Levie and Autio however, came to a more nuanced result. They took a deeper look at the particular interplay between the regulatory burden and the rule of law and its effects on strategic entrepreneurial decisions. Referring, amongst other unities of analysis, to an individual's decision to enter into business and, conceptually, to Signaling Theory, they assumed that individuals, who aim to profit most from their decisions, make their decisions in light of how they perceive the influence of institutional factors within society in relation to their activities. Similar to Mayer-Schönberger's understanding of a regulation shifting costs between different societal groups, the way how entrepreneurs perceive these factors regulates "the distribution of profits between stakeholders and, thus, the accumulation and approbiability of returns to entrepreneurial efforts."[135] Levie and Autio concluded a further conceptual dimension from this: their findings confirmed, firstly, the already known assumption that a "lighter regulatory burden (is) associated with a higher rate and relative prevalence of strategic entrepreneurial entry (word in brackets added by the author)."[136] However, the new finding was that rule of law "moderates this effect such that regulation has a significant effect on strategic entry only when rule of law is strong."[137] Instead of a weaker rule of law, as considered by Hartog et al., Levie and Autio thus suggest that a stronger rule of law enables entrepreneurship, under the condition that the regulatory burden is low.

In order to explain this suggestion, Levie and Autio generally considered four different types of interrelationships: First, if the rule of law is weak and the regulatory burden is heavy, corrupt officials get the opportunity to siphon off entrepreneurial rents; even if corruption is low, strategic entrepreneurs are more likely to interact with officials than non-strategic entrepreneurs and, thus, run a higher risk of being regulated heavily. Second, if the rule of law is weak and the regulatory burden is light, corrupt officials have fewer opportunities to siphon off entrepreneurial rents; however, entrepreneurs are less able to defend their own interests against other private parties by means of law. Third, if the rule of law is strong and the

135 See Levie and Autio, ibid., p. 1395.
136 See Levie and Autio, ibid., p. 1392.
137 See Levie and Autio, ibid., p. 1392.

regulatory burden is heavy, officials have fewer opportunities to siphon off entrepreneurial rents and entrepreneurs are able to defend their interests against other parties by legal means; however, they must pay the costs resulting from a heavy (effective) regulation. Consequently, Levie and Autio promote the fourth case as the best solution; if the rule of law is strong and the regulatory burden is low, entrepreneurs do not end up paying for corruption costs resulting from heavy regulation, but they also have sufficient legal means to defend their interests.[138] Even if their study referred to the distribution of profits between entrepreneurs and employees and, thus, to the choice of being a potential employer or an employee,[139] they draw a more general conclusion as: "Bureaucracy and red tape hamper entrepreneurial growth and divert scarce resources of potentially high-growth entrepreneurial firms away from their core business. Regulations, then, can adversely affect the prevalence and anatomy of entrepreneurial activity, particularly in countries in which the rule of law is respected."[140] Thus, in their opinion, if the regulatory burden is low, high legal certainty not only enables innovative large companies, but also small and middle-sized companies.

bb) Conditioning further legal certainty as a promoting factor for entrepreneurial activity

These results lead back to Mayer-Schönberger's approach. He considers a strong rule of law as an incentive for entrepreneurial activity. He argues that in light of the many uncertainties entrepreneurs are confronted with, they generally prefer to precisely know what the law expects from them. In Mayer-Schönberger's opinion, this knowledge would enable them to calculate their legal risks and associated costs. From this point of view, "the role of the legal system in facilitating entrepreneurial activity is to reduce the uncertainties that entrepreneurs perceive."[141] Mayer-Schönberger refers, similarly to Levie and Autio, to the Expected Utility Theory. How-

138 See Levie and Autio, ibid., pp. 1400 and 1401.
139 See Levie and Autio, ibid., pp. 1395 and 1396.
140 See Levie and Autio, ibid., p. 1411.
141 See Mayer-Schönberger, ibid., pp. 177 and 178; cf. also Kloepfer, Law enables Technology – About an understimated function of environmental and technology law, p. 417 and 418.

ever, he emphasises that the focus should be on how the law may play a decisive role in entrepreneurial risk calculation: In light of the individually different capabilities of evaluating risks, Mayer-Schönberger clarifies, at first, that more legal certainty does not necessarily lead to better entrepreneurial decisions but, at least, to more entrepreneurial activities. Second, in light of empirical findings demonstrating that individuals become more risk-averse the higher the potential payoff is, he suggests to increase legal predictability if entrepreneurs face high benefits or costs. Third, since individuals are more risk-averse when they evaluate potential benefits and more risk-taking regarding possible losses, he proposes "that lawmakers should focus on making legal rules more certain for financial benefits offered to entrepreneurs, like subsidies, rather than costs, like taxes".[142] He concludes that this perspective would enable the regulator to enhance entrepreneurial activity without decreasing protection, i.e. increasing costs, for third parties.[143]

c) Interim conclusion with respect to the principle of purpose limitation

So far, there appears to be a conflict. In the first instance, the principle of purpose limitation is principally open toward innovation because it leaves data controllers enough room to find the most cost effective way of applying the principle. However, in the second instance, the principle of purpose limitation decreases legal certainty and therefore fails in enhancing entrepreneurial activity. However, the previous considerations allows us to come to the conclusion that there are different hypotheses regarding the interplay between the principle of purpose limitation and data-driven innovation:

First, legal certainty acts as an incentive for entrepreneurs to apply the law, so long as the regulatory burden does not turn red tape. Whether this is the case or not with respect to the principle of purpose limitation depends on its interpretation and application in the specific case. Second, the higher the potential payoff for entrepreneurs is, the better legal certainty can act as an incentive to apply the principle of purpose limitation. This means that mechanisms clarifying how to apply the principle of purpose

142 See Mayer-Schönberger, ibid., pp. 179 and 180.
143 See Mayer-Schönberger, ibid., p. 180.

limitation only work better the more the data controllers potentially stand to lose or gain. The first might be the case if the penalties for non-compliance with the principle of purpose limitation are so high that the controller would consider its execution as a real loss. The second might be the case if the controller is going to break through in gaining users, customers or financial investors for their product, service or enterprise and these parties require, in exchange for giving data controllers their trust (i.e. personal data, money or investment), an assurance that the controller is applying the law (the principle of purpose limitation). This second case refers to the so-called competitive advantage of data protection law:[144] Users may only disclose their data to the data controller or customers may only pay for the product if certain data protection principles are met. Financial investors might verify whether the data controller has complied with data protection law, similarly to compliance with copyright law, as a condition for their investment. Indeed, there is little scientific evidence to what extent users, customers, or investors really expect such a compliance with data protection law. However, there is at least a study which demonstrates that users prefer products from online merchants with better privacy policies even if they have to pay a higher price for the product.[145] In any case, so long as a user or customer base does not yet constitute a real asset for the data controller or it does not need an external investment, these requirements do not serve an incentive per se. However, the moment where these factors constitute an asset for the controller, the second hypothesis becomes relevant: Since potential gains serve better than potential losses as incentive, the legislator should focus more, if it had to choose, on increasing legal certainty enabling entrepreneurs to exploit a competitive advantage than on penalties.

144 See, instead of many others, the ”Statement by Vice President Neelie Kroes, on the consequences of living in an age of total information’“ from the 4th of July 2013, retrieved on the 10th of March 2016 from http://europa.eu/rapid/press-release_MEMO-13-654_en.htm.

145 See Nissenbaum, Privacy in Context, p. 106 referring to Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. 2007. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. Paper presented at the 6th Workshop on the Economics of Information Security (WEIS), Carnegie Mellon University, Pittsburgh, PA, p. 35.

II. Data protection as a risk regulation

After having illustrated how economic models about innovative entrepreneurship provide links for doing research on the regulation of innovation, this sub-chapter draws the attention to the other side of the regulation of data-driven innovation, i.e. the protection against the risks. In the preceding considerations, the terms "risks", "dangers", "threats" and "harms" were already mentioned frequently, even if, however, rather casually. The following considerations clarify the meaning of these terms and how they serve, conceptually, as links for regulation.

1. Risk terminology oscillating between "prevention" and "precaution"

Legal scholars stress the function of data protection law as a regulation of risks.[146] And many data protection sources indeed aim to regulate risks caused by the processing of personal data. The revised OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data define, for example, its scope of application by referring to personal data as "which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties."[147] With respect to the EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the movement of data (Data Protection Directive), the Article 29 Data Protection Working Party stresses that the risk-based approach is "not a new concept, since it is already well known under the current Directive 95/46/EC."[148] Indeed, in several provisions, the Data Protection Directive explicitly refers, for instance, to "the risks represented by the processing" (regarding data security under Article 17), to "specific risks to the rights and freedoms of data subjects" (regarding prior checking under Article 20), and to the proportionality test (general clause

146 See Kuner et al., Risk management in data protection; Costa, Privacy and the precautionary principle; Gellert, Data protection: a risk regulation? Between the risk regulation of everything and the precautionary alternative.

147 See OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data in Article 2.

148 See the Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, p. 2.

for the controller's legitimate interests under Article 7 lit. f) that is typical for risk regulation regimes.[149] In the forthcoming General Data Protection Regulation (GDPR), risks play an even more important role, in particular, with respect to the so-called risk-based approach. Veil categorizes the multitude of terms referring to the risk-based approach and its legal consequences. For example, while one category referring to high risks can lead to the application of specific requirements, another category referring to low risks may result in the exclusion of requirements; yet another category determines, for instance, the extent and manner of how data controllers must implement measures protecting against risks.[150] In this last regard, Article 24 of the General Data Protection Regulation provides for a central provision stating as:

> "*Taking into account the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for the rights and freedoms of individuals, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. These measures shall be reviewed and updated where necessary.*"[151]

The Article 29 Data Protection Working Party stresses that such a risk-based approach "goes beyond a narrow 'harm-based-approach' that concentrates only on damages and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the personal concerned by the processing in question to a general societal impact (e.g. loss of social trust)."[152]

From a historical perspective, indeed, it is not a new idea to focus on risks, thus, on a moment before a danger occurs. The idea behind such a temporal extension of protection is that a protection for an individual, who might be the subject of the use of information, could be too late if he or she was only able to claim against the specific use of that information after it had been collected. Legal scholars had recognized, very early in the discussions about data protection, as well as privacy that a protection against

149 With respect to the last aspect, see Kunert et al., ibid., p. 98, as well as Costa, ibid., p. 19.

150 See Veil, GDPR: Risk-based approach instead of rigid principle of prohibition, pp. 351 and 352.

151 Cf. already the Article 29 Data Protection Working Group, Opinion 3/2010 on the principle of accountability.

152 See the the Article 29 Data Protection Working Group, Statement on the role of a risk-based approach in data protection legal frameworks, p. 4.

the collection of the data (providing the basis for the information), can instead be more effective. For instance, in 1969, Miller highlighted that "the most effective privacy protection scheme is one that minimizes the amount of potentially dangerous material that is collected and preserved; a regulatory scheme that focuses on the end use of the data by governmental or private systems might be a case of too little, too late."[153] The reason for this fear is that once information is spread, in metaphorical words, the cat is led out of the bag, and it is difficult to get it back. Once the State or a private entity knows something about somebody else, it can base its decisions (with all possibly negative consequences for the individual concerned) on this knowledge.[154] Thus, from a regulatory perspective, it seems to be more difficult to enforce the State or a private entity not to base its decisions on this knowledge than to regulate the collection of the personal data as the source of this informational risk.

Such a risk-related regulatory approach plays also an important role in Germany. Costa refers to the so-called precautionary principle that was first formalized by Germany during the 1970's in environmental law;[155] and Gellert quotes the "pioneering" data protection legislation established by the German Land Hessen that "implicitly frames data protection as a risk regulation regime since one of its purposes is to: 'safeguard the constitutional structure of the state (…) against all risks entailed by automatic data processing'."[156] The German legal scholar Roßnagel draws the attention to the regulator's protection instruments resulting from such a risk approach. He highlights the principle of data minimization as an example for the precautionary principle because it extends, similar to the minimization principle in environmental law, the protection provided for by preventative means by adding precautionary means. In his opinion, the requirement of data minimization particularly goes beyond the *necessity requirement* (i.e. that the data processing must be necessary for achieving the purpose of the

153 See Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, p. 1221.

154 See Grimm, Data protection before its refinement, p. 586.

155 See Costa, ibid., p. 4, referring to Olivier Godard, "Introduction générale", in: "Le principe de précaution dans la conduite des affaires humaines" (Paris: Editions de la Maison des sciences de l'homme Institut National de Recherche Agronomique, 1994), p. 25.

156 See Gellert, ibid., p. 5, referring to Lee A Bygrave, Data Protection Law—Approaching Its Rationale, Logic, and Its Limits (Kluwer, The Hague; London; New York 2002), 39, at 5.

processing intended) because the latter depends on a specific purpose while the first questions the purpose per se. Thus, the principle of data minimization does not require asking whether or not the processing is necessary for a given purpose but whether the purpose as such can be formulated more narrowly in order to minimize the data collection as a whole. In light of this, Roßnagel differentiates between both principles pursuant to their range of protection: while the necessity requirement serves the prevention of dangers, the requirement of data minimization is a means of precaution.[157] This consideration leads to the question of how to differentiate, actually, between prevention and precaution.

2. Sociological approaches defining "dangers" and "risks"

The German legal scholar Jaeckel considers the difference between prevention and precaution as corresponding to the question of how to differentiate between dangers and risks.[158] Indeed, while there is common sense in the meaning of an actual harm or damage, e.g. "a loss to a person or their property"[159], the precise meaning of terms like danger and risk referring to a potential harm (i.e. overall threat) is less clear. Jaeckel gives an overview about sociological and legal conceptions of how to differentiate between dangers and risks.[160] From a sociological perspective, she highlights the concepts proposed by Evers and Novotny, on the one hand, and Luhmann, on the other hand.

Evers' and Novotny's starting point is to define "risk" as a term seeking to make dangers calculable. Thus, the specific knowledge about the probability and severity of a threat turns dangers into risks.[161] Subsequently, Evers and Novotny draw the attention to the normative dimension of risks.

---

157 See Roßnagel, The Requirement of Data Minimization, pp. 43 to 45.

158 See Jaeckel, Differentiating between Danger and Risk, p. 117; Prevention of Danger through Law and Legal Conceptualization of Risk, p. 70.

159 See, for example, Costa, ibid., p. 14.

160 See Jaeckel, Prevention of Danger through Law and Legal Conceptualization of Risk, pp. 49 ff.

161 See Jaeckel, ibid., pp. 51 and 52, by referring to Evers and Novotny, Umgang mit Unsicherheit, Suhrkamp 1987, Berlin; cf. also Gellert, ibid., pp. 7 and 13, referring to Patrick Peretti-Watel, La société du risque (Repères. La Découverte, Paris 2010); Olivier Borraz, Les politiques du risque (Presses de Sciences Po, Paris 2008), Jenny Steele, Risks and Legal Theory, vol 68 (Hart Publishing, Oxford,

They stress that the difference between dangers and risks depends on its general perception in today's society. For example, citizens express their concerns and fears about a certain issue like environmental pollution or state surveillance based on an abuse of personal data because there is a societal consensus that environmental health or privacy or autonomy in a democratic civil society is a value. Thus, the moment citizens perceive a non-calculable threat for environmental health, their privacy or autonomy, this perception can turn a risk back to a danger for these values. Jaeckel stresses Evers' and Novotny's conclusion that mathematic and system-analytical methods of calculating risks alone can hence not explain the treatment of uncertainties in a society; instead, this treatment also depends on its normative expectations.[162]

Luhmann, in contrast, differentiates between dangers and risks pursuant to the question of who is considered as responsible for the (potential) harm. If the harm is considered as resulting from an external factor, Luhmann refers to the term "danger"; instead, there is a risk if the harm is considered as resulting from a human decision. Jaeckel considers this perspective as interesting from a legal viewpoint because it illustrates that not only decisions which lead to active action but also decisions not to act, may in itself be considered as causing risks. For example, the prohibition of a certain medicine against a certain disease can avoid risks resulting from unwanted side effects but, simultaneously, create or increase the risk caused by the disease itself. This nature of decisions as a two-sided sword

---

UK; Portland, Oregon 2004) 21, Jacqueline Peel, Science and Risk Regulation in International Law (Cambridge University Press, Cambridge, UK 2010) 79–80.

162 See Jaeckel, ibid., pp. 51 and 52, by referring to Evers and Novotny, Umgang mit Unsicherheit, Suhrkamp 1987, Berlin; cf. also van Dijk, Gellert and Rommetveit, A risk to a right? Beyond data protection risk assessments, p. 13, referring, amongst others, to Felt U,Wynne B, Callon M, Gonçalves ME, Jasanoff S, Jepsen M, et al. Taking European knowledge society seriously (report of the expert group on science and governance to the science, economy and society directorate, directorate-general for research). Luxembourg: European Commission; 2007, as well as Irwin A,Wynne B, editors. Misunderstanding science? – the public reconstruction of science and technology. Cambridge: Cambridge University Press; 1996; see, regarding the German perspective, at Forum Privatheit, White Paper – Data Protection Impact Assessment, pp. 29 and 30.

leads to the result that potential negative effects must always be weighed against potential positive effects in order to determine the overall risk.[163]

In any case, Jaeckel comes to the conclusion that both concepts do actually not correspond to approaches developed so far in (German) legal literature: Luhmann's concept does not help, in her opinion, determine the real risk or danger and, therefore, does not answer the question of which protection instruments are needed in order to establish against real risks or dangers. And the concept by Evers and Novotny contradicts the legal discussion considering the relationship between danger and risk in the reverse direction. In Germany, at least, the legal discussion considered that a danger was the calculable threat, whereas a risk was considered as an uncertain threat that could not comprehensively be grasped.[164]

3. German legal perspectives: Different protection instruments for different types of threat

In Germany, initially focusing on police law, the debate centered, for more than a century, on the notion of *prevention of danger*. In contrast, the legal debate started to develop the notion of *precaution against risks* in the 1980's, holding the reference to this relatively new term as a necessary answer to the scientific and technological progress.[165] This progress produced a new type of threat that did not appear to fit to the classic understanding of a *danger*. The debate discovered, in particular, the following characteristics: First, these threats only become apparent after a long period had lapsed and/or when it is looked at from a global perspective; second, only the combination of several issues, which are, per se, not risky if they remain a singular phenomenon, together cause a threat; or third, a threat is indeed extremely unlikely but runs the risk of causing an ex-

163 See Jaeckel, ibid., pp. 53 to 56, referring, amongst others, to Luhmann, Soziologie des Risikos, pp. 30 ff, as well as, ibid., Die Moral des Risikos and das Risiko der Moral, in: Bechmann, Risiko und Gesellschaft, pp. 327 and 331.

164 See Jaeckel, ibid., pp. 52 as well as 55 and 56.

165 See Jaeckel, ibid., p. 57, referring, amongst others, to decisions of the Prussian Higher Administrative Court (Preußisches Oberverwaltungsgericht) as well as to Murswiek, Die staatliche Verantwortung für die Risiken der Technik, p. 80, and Kloepfer, Umweltrecht, 1. Auflage 1989, p. 45 cip. 46.

tremely severe and irreparable harm.[166] In light of the perception of such risks in society as a new form of threat, the legislator started to use the term in law, and the legal discussion started to react to this term by clarifying its precise meaning and extent.

a) Protection pursuant to the degree of probability

At first, the legal discussion elaborated on a three-layered model differentiating between dangers, risks, and remaining risks combined with different legal consequences: While a regulator had to strictly prevent a danger, it could only minimize a risk; and there also is a *remaining risk* that had to be accepted without protection against it. On the basis of this differentiation, this model defined the term *danger* as a situation that may turn, with sufficient probability, into a harm for a specific object of protection if nobody were to stop this causal chain. Certainty about the harm, thus, is not necessary; however, the concept of harm as being an only possible threat was considered as insufficient for regulation. Between these two poles, i.e. certainty and possibility, the regulation depended on the probability of the harm. Indeed, there is no fixed probability required, instead, the following balancing exercise had to be carried out: The more severe the potential harm is, the less probable it had to be in order to create a state duty of protection, and vice versa. Indeed, the moment the existence of a danger could be determined, the State had to prevent it, irrespective of how much effort had to be spent on prevention; in the worst case scenario, the State or any other party had to refrain from the action or decision that caused the danger.[167]

In contrast to such a prevention of dangers, precaution against risks takes place before preventative measures can protect against threats. Pursuant to the three-layered model, a situation is risky if harm is possible but the methods elaborated with respect to a danger cannot determine its probability. This might be the case because of one of the following three reasons, which were mentioned previously: First, the negative effects of an action or decision may take place too far in the future; second, its causality is hard to determine because there are too many factors leading to the po-

166 See Jaeckel, ibid., p. 58 with reference to Murswiek, Die staatliche Verantwortung für die Risiken der Technik, p. 80.

167 See Jaeckel, ibid., pp. 57 to 60 with further references.

tential harm; or third, its probability is just too low. In light of the lower threat of a risky situation than of a dangerous one, the regulator does not have to prevent the threat as a whole but only to minimize it. Furthermore, this duty depends on the technical possibilities, as well as the proportionality between efforts and utility. Another difference between prevention of a danger and precaution against risks is that the individual concerned has a subjective right to protection only against dangers but not against risks. Finally, this three-layered model acknowledged a third category of threat, i.e. *remaining risks* that must be socially accepted without having protection measures against it. This results from the fact that no technology can guarantee full protection against all threats imaginable. A duty of protection against such threats would therefore be disproportionate and lead to a prohibition of technology development.[168]

Jaeckel confirms that this three-layered approach brought to light the issue that there are different kinds of threats that require different protection instruments. However, the problem of this model was that it only superficially provided a clear differentiation between dangers, risks, and remaining risks. In fact, it was hardly possible to precisely determine which situation bears a danger, or a risk, or only a remaining risk. This uncertainty was problematic because the three-layered model tied precise legal requirements to these three categories: If one type of threat (i.e. danger) requires preventative protection measures, another type of threat (i.e. risk) requires minimizing measures, only, and a third type of threat (i.e. remaining risk) requires no protection at all, then its differentiation should be clear.[169] In order to minimize this problem, legal scholars had therefore proposed, a two-layered model that mainly differentiated between dangers and risks, on the one hand, and remaining risks, on the other. This two-layered model considered a risk as the umbrella term and a danger as a specific type of risk. From this perspective, the term *risk* meant all possible threats, whereas a danger is a threat with a certain probability.[170] Jaeckel affirms that this concept enables one to tie different proportionate protection instruments to different types of threats, without drawing an artificial and over-formalistic line of distinction. However, in her opinion, it would nevertheless be helpful to clearly differentiate between dangers and

168 See Jaeckel, ibid., pp. 60 and 61 with further references.
169 See Jaeckel, ibid., pp. 62 to 63.
170 See Jaeckel, ibid., p. 66 referring to Murswiek, Die staatliche Verantwortung für die Risiken der Technik, pp. 80 ff. and 335 ff.

risks in order to choose the adequate and proportionate protection instruments.[171]

b) Protection pursuant to the available knowledge in linear-causal and non-linear environments

Tying into the conceptual approaches developed by Di Fabio and Ladeur, Jaeckel finally comes to the conclusion that the actual difference between dangers and risks consists in the methodologies for (administrative) "decisions under uncertainty":[172] A danger refers to a type of threat that is, based on individual and societal experience, which is already known so that the State is able to react to it with an experienced set of methodologies. In contrast, the term "risk" refers to knowledge that is not certain. This perceived uncertainty results from the conceptual shift from a linear and causal approach to a non-linear and dynamic approach in understanding the world.[173] In a non-linear dynamic world, "the loose connection between cause and effect requires new concepts for actions or decisions based on uncertain knowledge: 'The connection between action and knowledge, which was made in the past through the term of danger, has to be made today, under the conditions of increased complexity and uncertainty, through the term of risk.'"[174] From this knowledge perspective, the main difference between a danger and a risk hence is that an objective observer having all the knowledge of the world is principally able to determine under which conditions a danger turns into harm; in contrast, regarding risks, there is no objective knowledge horizon about the outcome of a risk, instead, there principally is only a subjective point of view. In Jaeckel's opinion, the regulator reacts to this paradigm shift (i.e. with respect to the knowledge uncertainties) by introducing, more and more, subjective elements into the law: First, by accumulating knowledge through the integration of expert groups and private entities and by stretching, second, these procedures from a time perspective, as well as by binding them to

171 See Jaeckel, ibid., pp. 69 and 70.
172 See Jaeckel, ibid., p. 77.
173 See Jaeckel, ibid., pp. 78 to 80.
174 See Jaeckel, ibid., p. 81, quoting Ladeur, The Environmental Law of the Knowledge Society: From the protection against dangers to the management of risks, p. 78.

procedural rules; and third, by acknowledging that the introduction of legal objectives, like broad legal terms and principles, corresponds with a certain limitation of the judicial review. If knowledge is exclusively subjective, then the Courts have to acknowledge this subjectivity and cannot substitute it by their own "objective" point of view. Indeed, Jaeckel stresses that this limitation of judicial review only applies insofar as there really is an uncertainty that limits the construction of an objective knowledge horizon.[175]

c) Interim conclusion: Fundamental rights determining the appropriateness of protection

With respect to the protection instruments, preventative measures thus seek to directly protect against dangers, i.e. linear-causal threats of sufficient probability for specific objects of protection. In contrast, precautionary measures react to the knowledge deficiencies resulting from dynamic and non-linear environments. They serve to maintain possibilities for action if there is, for example, no objective proof for a causal connection between a certain action and a later harm for a specific object of protection. Therefore, they often refer, at first, to informational measures rather than control. Jaeckel advocates that this conceptual difference enables the regulator to choose, with respect to the particularities of a certain area of life, the proportionate protection instruments for the different types of threats.[176] Indeed, the choice for the proportionate protection instruments consists, of two different questions: The first question refers to the duty of protection of the State. This question posed is: which type of threat requires which protection instrument, in other words, whether preventative or precautionary measures are necessary in order to (finally) avoid a potential harm. The answer depends, similarly for the actual harm, on the fundamental rights of the individuals concerned or other constitutional guarantees (e.g. environmental protection under Article 37 of the European Charta of Fundamental Rights).[177] The second question posed is:

175 See Jaeckel, Differentiating between Danger and Risk, p. 120.
176 Jaeckel, ibid., p. 123.
177 See Jaeckel, Duties of Protection in German and European Law, pp. 85 to 88 as well as 165 and 166; cf. also van Dijk, Gellert and Rommetveit, A risk to a right? Beyond data protection risk assessments, pp. 17 and 18.

whether the protection instrument established in order to fulfill a State duty of protection is proportionate or not. The answer to this question does not only refer to the fundamental rights of the individual concerned, but also on the fundamental rights of the entities (e.g. entrepreneurs), which must apply this protection instrument. Thus, this answer therefore depends on the balancing exercise between the opposing fundamental rights. This balancing exercise may result in the fact that the prevention of a certain action (e.g. its prohibition) that leads to a risk (not a danger) would be disproportionate. In contrast, a precautionary measure, which only seeks to gather information in order to potentially discover a danger is proportionate. The reason is that the requirement to gather information infringes the fundamental rights of the entrepreneur less, than the prohibition of its actions.[178]

4. Searching for a scale in order to determine the potential impact of data protection risks

The essential point here is that this doctoral thesis does not purport to decide which definition of risks and dangers is appropriate. However, its aim is to illustrate that there are different kinds of threats that require different protection instruments. Therefore, this thesis mainly refers to the term, "threat" or uses both terms "risks" and "dangers", synonymously, unless stated otherwise. In conclusion, amongst these threats, there are particular situations where there is insufficient knowledge in order to specify an object of protection threatened by a certain action or to determine a causal link between this action and a potential harm. Costa describes the precaution against these kind of threats, giving yet another definition, as based on "hypotheses that have not been scientifically confirmed", in contrast to the prevention of "identifiable risks".[179] In other words, "while the prevention is the remedy against the exposure with regard to a known harm, precaution is meant to avoid the mere possibility of suffering harm or

178 See Jaeckel, Duties of Protection in German and European Law, pp. 85 to 88 as well as 165 and 166; Dietlein, The Doctrine of Duties of Protection of Basic Rights, pp. 105 to 109; cf. Kuner et al., ibid., p. 98; see below in more detail regarding the duties of protection point C. I. b) The effects of fundamental rights on the private sector.

179 See Costa, ibid., p. 15.

loss."[180] From this point of view, both approaches of protection, i.e. prevention of known risks and precaution against unknown risks, do not exclude each other but, instead complement each other. Thus, when the risk is "known" or "identified", this is the essential moment when there is a switch from precautionary to preventative measures. It is at this moment, when the protection instruments do not primarily aim to identify a risk anymore but instead to prevent it.[181] Such a differentiating approach is particularly important if protection measures shall not forbid all future innovations, but instead, the protection instruments applied shall be proportionate, respecting the conflicting constitutional positions, such as fundamental rights.[182]

However, the most urgent challenge of such a "risk-based" approach applied to data protection law is the question of how to determine the potential harm, i.e. the object of protection that actually is threatened by a certain action or decision. Many scholars stress that beyond common sense, i.e. that not only material but also immaterial harm must be considered, there is little agreement on how to determine the corresponding threats.[183] This is a desperate situation for a regulation aiming to protect against threats caused by the processing of personal data. The reason is that effective protection is possible only if it is clear which of these threats are legally relevant. The answer to this general question may lead, in particular, to further answers to more specific questions, such as: what kind of information is actually needed in order to discover threats; which threats must be accepted without having protection instruments against it; how to avoid "rabulistic games" with numbers determining the probability and severity of threats; and thus, how to avoid, firstly, that the risk-based approach undermines rights and duties provided for by fundamental rights and, second, risk management processes provided for by ordinary data protection law "may be perverted into a self-legitimation exercise that serves no other purpose than that of managing operational and reputational

180 See Costa, ibid., p. 5.
181 Cf. Costa, ibid., pp. 2, 5, and 14 to 18.
182 See the criticism of the precautionary principle provided for by data protection, in particular, at Thierer, Privacy Law's Precautionary Principle Problem.
183 See, for example, Kuner et al., ibid., p. 97; Center for Information Policy Leadership, The Role of Risk Management in Data Protection – Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy, p. 13.

risks, and which, ultimately, is itself a risk to the management of (primary) risks."[184]

III. Theories about the value of privacy and data protection

In order to answer this question, it is necessary to determine the overall objective that data protection actually serves. It is necessary to stress that this chapter does not yet precisely differentiate between theories, concepts, or approaches of privacy, on the one hand, and data protection, on the other. Both terms are therefore (still) synonymously used.[185]

1. The individual's autonomy and the private/public dichotomy

Without requiring a complete and detailed description of each single theory on this matter, Nissenbaum provides, in her book *Privacy in Context*, an overview about "predominant themes and principles, as well as a few of the well-known theories that embody them."[186] In doing so, Nissenbaum organizes these theories into two categories: First, theories that consider privacy as related or even necessary for further moral or political values; and, second, theories that attribute the legitimacy question of privacy to the individual's capacity to control a certain "private zone".[187]

With respect to the first category, i.e. theories connecting privacy with further moral or political values, the individual's autonomy plays an important role. There can be several threats endangering the autonomy of individuals who are concerned by the processing of personal data. Quoting Stanley Benn, Nissenbaum defines autonomy as "self-determination embodied in the individual 'whose actions are governed by principles that are his own' and who 'subjects his principles to critical review, rather than

184 See Gellert, ibid., pp. 14 to 17, referring, with respect to the quote, to Michael Power, The Risk Management of Everything – Rethinking the Politics of Uncertainty (Demos, London 2004), p. 19.

185 See, for example, in relation to EU law, the discussion about the terminological (and conceptual) shift from "privacy" to "data protection" at González-Fuster, The Emergence of Data Protection as a Fundamental Right of the EU.

186 See Nissenbaum, Privacy in Context, p. 13.

187 See Nissenbaum, ibid., p. 73.

taking them over unexamined from his social environment'".[188] Nissenbaum acknowledges that such an understanding of autonomy might indeed be endangered in light of the thought experiment proposed by Jeffrey Reiman called the "informational panopticum":[189] Similar to Jeremy Bentham's panoptic prison, the life of an individual trapped in an informational panopticum can be observed from one single point of view. Given the current development of collection, aggregation, and analysis of personal data, Nissenbaum considers such a thought experiment not as unreasonable.[190] Instead, she delves deeper into the four types of risks that Reiman considers for an individual's autonomy caused by the informational panopticum: "risks of extrinsic and intrinsic losses of freedom, symbolic risks, and risks of 'psycho-political metamorphosis'".[191]

An extrinsic loss of freedom arises when an individual suffers from negative decisions by third parties due to information third parties are able to gather about the individual. For example, an employer receives information (that could be true or untrue) about the work performance of a potential employee and decides not to give the potential employee the job based on this information. An intrinsic loss of freedom results from anteceding self-censorship because the individual fears such potential external losses and therefore omits behaviors that could lead, once somebody else is informed about it, to a negative decision made by others. The symbolic risk refers to a lack of institutional bodies and concepts affirming the right of the individual to act autonomously without having to fear losses of their freedom. The fourth risk of psycho-political metamorphosis finally "follows Reiman's speculation that if people are subjected to constant surveil-

188 See Nissenbaum, ibid., p. 81 quoting Stanley Benn (1971), Privacy, Freedom and Respect for Persons, in: Privacy, ed. J. R. Pennock and J. W. Chapman, New York: Atherton Press, pp. 1 to 27 (p. 24), reprinted in Philosophical Dimensions of Privacy: An Anthology, ed. F. Schoeman. Cambridge: Cambridge University Press, 1984, pp. 223– 244.

189 See Nissenbaum, ibid., quoting Jeffrey Reiman (1995), Driving to the Panopticum: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, Santa Clara Computer and High Technology Law Journal 11(1): pp. 27 to 44 (p. 33).

190 See Nissenbaum, ibid., p. 75 referring to Jeffrey Bentham (1995), The Panopticon Writings. M. Bozovic, ed. London: Verso.

191 See Nissenbaum, ibid., pp. 75 and 76 referring to Jeffrey Reiman (1995), Driving to the Panopticum: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future, Santa Clara Computer and High Technology Law Journal 11(1): pp. 27 to 44 (p. 42).

lance, they will be stunted not only in how they act, but in how they think. They will aspire to a middle-of-the-road conventionality — to seek in their thoughts a 'happy medium.'"[192] From this perspective, a right to privacy and/or data protection protecting against these threats indeed serves an individual's autonomy.[193] However, Nissenbaum concedes that autonomy does not require that individuals are totally free from any social influence. It is a thin line to draw between coercion, manipulation, and deception, on the one hand, and respecting the individual's autonomy, on the other. In particular, there is no proof that the processing of personal data leads, in general and automatically, to harm for the autonomy, but only that it may.[194]

The preceding considerations about the individual's autonomy lead to the second value of privacy, for human relationships. Several theorists stress the value of privacy which enables individuals to decide who they want to trust or not, i.e. it is the individuals who decide who they want to share personal information with. Autonomy therefore is an important precondition for developing relationships.[195] Finally, and equally related to the concept of autonomy, Nissenbaum refers to another scholar who stresses the importance of privacy for society as a whole: Priscilla Regan considers and promotes the notion that privacy enables individuals to decide on which aspects of their personal life they want to place in the background, distinguishing them from others, and which aspects they choose to share with others in order to signal their commonalities. This ability is an essential pre-requisite for being a citizen in a democracy, which becomes particularly obvious with respect to the freedom of association. However, there are further constitutional positions related to or even dependent on privacy such as the fundamental right to anonymous speech or the institution of the secret ballot. These examples make apparent that privacy per se must not be at the complete disposal of individuals, who use their privacy or may abandon it, but has to be considered as a collective good. Regan

192 See Nissenbaum, ibid.

193 Cf. Nissenbaum, ibid., p. 81.

194 See Nissenbaum, ibid., p. 83 and 84.

195 See Nissenbaum, ibid., pp. 84 and 85 referring to Charles Fried (1986), Privacy: A Moral Analysis, Yale Law Journal 77(1): pp. 475– 493 (pp. 477 ff.) as well as Ferdinand Schoeman (1984), Privacy and Intimate Information, in: Philosophical Dimensions of Privacy: An Anthology, ed. Ferdinand Schoeman, Cambridge University Press, pp. 403 to 418 (p. 408) and James Rachels (1975), Why Privacy Is Important, Philosophy & Public Affairs 4(4): pp. 383 to 423 (p. 326).

advocates that this nature of privacy "as a non-excludable, indivisible collective good like clean air and national defense" gives a good reason for concluding that the legislator should regulate privacy by public law and not completely leave it to mechanisms of the private market.[196]

The second category of theories equally considers privacy as important for an individual's ability to avoid scrutiny, approbation and hence, in more general words, threats for his or her autonomy. However, these theories consider privacy and how it is conceptualized by the preceding theories as too broad and therefore focus on its function to define a specific "private zone". From this point of view, all concepts of privacy can only refer to a private realm but not to the public sphere. Nissenbaum calls this approach the "private/public dichotomy".[197] Pursuant to her analysis, there are three basic strands defining this private/public dichotomy. The first strand defines the dichotomy by distinguishing between private and public "actors". The second strand defines it by distinguishing between private and public spaces. And the third strand refers to the distinction between private and public information.[198] Pursuant to these theories, a right to privacy shall exist only for these private zones, otherwise the value of privacy and, thus, protection for it is unclear.[199]

2. Criticism: From factual to conceptual changes

Nissenbaum criticizes all of these approaches. With respect to the second category, theories referring to the private/public dichotomy, in her opinion, these theories are not problematic as such, but are not useful in today's world for elaborating on a normative concept of protection. She argues: "Although, in the past, it might have served as a useful approximation for delineating the scope of a right to privacy, its limitations have come to light as digital information technologies radically alter the terms under which others – individuals and private organizations as well as government – have access to us and to information about us in what are traditionally understood as private and public domains. In the period before such

196 See Nissenbaum, ibid., p. 87 referring to Priscilla Regan (1995), Legislating Privacy, Chapel Hill: University of North Carolina Press, pp. 226 and 227.
197 See Nissenbaum, ibid., pp. 89 and 90.
198 See Nissenbaum, ibid., pp. 91 ff.
199 See Nissenbaum, ibid., pp. 98.

technologies were common, people could count on going unnoticed and unknown in public arenas; they could count on disinterest in the myriad scattered details about them."[200] Today, in contrast, personal data can be, once it is collected in a certain context, permanently stored and can always be analyzed and used in another context. In light of this "always-possible context change", the linear private/public dichotomy, hence, does not serve as a useful criterion reliably distinguishing, for example, between private and public spaces or private and public information anymore.[201] However, the theories described before, which focus on the value of privacy in relation to further moral or political values, in particular to autonomy, do not provide reliable criteria in order to distinguish various forms of data processing from others either. Nissenbaum summarizes, in particular, the following weaknesses of these theories as: "One recurring skeptical challenge, for instance, cites the lack of concern many people seem to demonstrate in day- to-day behaviors, contradicting claims that privacy is a deeply important moral and political value that deserves stringent protection. Another is the clearly evident cultural and historical variation in commitments to privacy, hard to explain if privacy is supposed to be a fundamental human right. A third points to the difficulty of resolving conflicts between privacy and other moral and political values, such as property, accountability, and security."[202]

The shortcomings of all these theories become, in Nissenbaum's opinion, most apparent in light of their inappropriate answers to the threats to privacy caused by modern Internet and Information technologies. The existing theories lead to the result that the public discourse discusses some of the new technologies with great anxiety even if they do actually not pose a significant risk to privacy. In contrast, existing concepts do not provide for sufficient protection measures against other technologies, which heavily put traditional understandings of privacy in question, only because their principles are "'blind' to essential elements and differences" of these technologies.[203] As a consequence of all these challenges, Nissenbaum finally develops her approach not by creating her own new principles of privacy, but rather by reacting to altered factual conditions and, thus, elaborating

200 See Nissenbaum, ibid., pp. 116 and 117.
201 Cf. Nissenbaum, ibid., pp. 113 ff.
202 See Nissenbaum, ibid., p. 14.
203 See Nissenbaum, ibid., pp. 103 and 104.

on the existing principles:[204] the framework of "contextual integrity".[205] One essential element of this approach is to specify conditions for the flow of personal information with respect to a certain context. From this point of view, a right to privacy is not a right to secrecy or to control of certain information, but to appropriate flow of information.[206]

Interestingly, Nissenbaum also heavily criticizes the purpose-based approach. However, before analyzing this criticism and, as a consequence, coming to the question of the relationship between a "context" in which the data processing (aka information flow) takes place and the "purpose" of this processing, the next paragraph delves deeper into the approach of contextual integrity. The reason is that this approach may help, once the question of the context-purpose-relationship is clarified, find an answer to the research question about the meaning and extent of the principle of purpose limitation.

3. Nissenbaum's framework of "contextual integrity"

Elaborating on her framework of contextual integrity, Nissenbaum underlines, as mentioned previously, that she does not want to substitute current intuitive principles of privacy. In contrast, she seeks to provide a concept, which functions better than current theories, in order to evaluate whether or not a certain flow of information infringes such intuitive principles of privacy. Pursuant to her framework, a certain use of information infringes "contextual integrity" only if it conflicts with "informational norms" that exist in specific contexts. These informational norms are specified by the

---

204 See Nissenbaum, ibid., p. 118 quoting Lawrence Lessig (1999), Code and Other Laws of Cyberspace, New York: Basic Books, p. 116 as: "This form of argument is common in our constitutional history, and central to the best in our constitutional tradition. It is an argument that responds to changed circumstances by proposing a reading that neutralizes those changes and preserves an original meaning... It is reading the amendment differently to accommodate the changes in protection that have resulted from changes in technology. It is translation to preserve meaning'"; cf. the same approach in German law, Grimm, Data protection before its refinement, p. 585, who differentitates between the over-arching aim specified by the object of protection of fundamental rights and the concept of protection that must be adapted, from time to time, to the changes of the environment.

205 See Nissenbaum, ibid., p. 14.

206 See Nissenbaum, ibid., pp. 127 and 239.

following factors: First, the corresponding context; second, the actors involved; third, attributes such as the type of information; and fourth, principles for the transmission of the information.[207]

Nissenbaum proposes the following explanations for these factors: the term "context" refers to "structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more."[208] By way of example, she names contexts such as health care, education, employment, religion, family, and the commercial marketplace.[209] The second factor, i.e. the type of information, can refer to the dichotomy between private and publically available information, but it is however, not restricted to these types. Instead, further types can equally be relevant. In this regard, Nissenbaum provides examples that friends might share intimate information amongst each other but not, for example, their salaries; in contrast, the same people might share the information about their salaries with their bankers or tax lawyers, but not the intimate information shared with their friends; similarly, the information exchange about religious affiliation might be appropriate amongst friends, but not between an employer and his or her employee; and finally, a physician might ask for medical information but not about the religious or financial matters of an individual.[210]

Correspondingly, the definition of the social role by the individual also depends on the context. For example, in a health-care context it is decisive in order to define the social norms, whether the doctor, receptionist, nurse, or bookkeeper receives certain types of information.[211] This example also points to the fourth factor, i.e. the transmission principle. Nissenbaum stresses that her framework of contextual integrity is not restricted to a binary transmission principle, such as having access or not having access to information. Instead, she stresses the point that there are several possible conditions governing how in a certain context, certain types of information might be shared amongst certain actors. For instance, there may be a principle of reciprocity for sharing information, such as amongst friends; or rights of receiving certain information; or duties of providing for certain

207 See Nissenbaum, ibid., p. 181.
208 See Nissenbaum, ibid., p. 130.
209 See Nissenbaum, ibid., p. 130.
210 See Nissenbaum, ibid., pp. 143 and 144.
211 See Nissenbaum, ibid., pp. 141 and 142.

information; or a right for individuals to determine by themselves the conditions of a certain information flow; there may be a principle requiring that information is shared voluntarily or consensually or based on the knowledge of the individual concerned ("notice") or on his or her permission ("consent"), or a combination of all or some of these conditions.[212] In any event, Nissenbaum stresses that "contexts are not formally defined constructs, but (…) are intended as abstract representations of social structures experienced in daily life. (…). In other words, the activity of fleshing out the details of particular types of contexts, such as education or health care, is more an exercise of discovery than of definition."[213]

Irrespective of whether this statement is correct or not, and supposing that the particularities of a specific context is fleshed out in detail, and its informational norms are determined, the next step in the framework of contextual integrity is to evaluate whether or not a certain flow of information challenges the corresponding norms and therefore violates its contextual integrity. Nissenbaum recognizes the fact that if all information flows that challenge an already existing norm were considered as violating its contextual integrity, the evolvement of new norms, i.e. change per se, would be problematic. In order to avoid a "lock-in effect" in entrenched norms that hinders new developments, Nissenbaum hence adds to her framework a normative component: the value of a specific context. In light of this component, new informational norms challenging existing ones "can be justified on moral grounds insofar as they support the attainment of general as well as context-based values".[214] Thus, coming from her approach that existing informational norms are presumed to be appropriate norms, she considers that new norms can also be justified, so long as they are more effective in supporting, promoting or achieving context-related values than existing informational norms.[215] These contextual values, in other words, purposes, objectives or ends hence play an essential role for evaluating whether or not a new informational norm within a given context violates the contextual integrity. Nissenbaum stresses, referring to Schatzki's "teleology", the function of these contextual values as necessary for any understanding of why individuals behave in certain contexts in a certain way, in more abstract words, why certain context-related infor-

212 See Nissenbaum, ibid., pp. 145 to 147.
213 See Nissenbaum, ibid., p. 134.
214 See Nissenbaum, p. 181 and pp. 158 ff.
215 See Nissenbaum, p. 181 and pp. 158 ff.

mational norms exist. She comes to the conclusion that even if "settling on a definitive and complete list of contextual values is neither simple nor non-contentious, the central point is that contextual roles, activities, practices, and norms make sense largely in relation to contextual teleology, including goals, purposes, and ends."[216]

4. Clarifying the relationship between "context" and "purpose"

Promoting this approach of contextual integrity, Nissenbaum also criticizes, as mentioned previously, the purpose-based approach. In her opinion, the principle of purpose limitation that consists of the two requirements, first, to specify the purpose of the processing of personal data and, second, to limit the later use of the data to the purpose initially specified, has "only indexical meaning".[217] She stresses that so long as there is no substantive criteria in order to specify a purpose, privacy and/or data protection laws "constitute a mere shell, formally defining relationships among the principles (that refer to the purpose of the data processing) and laying out procedural steps to guide information flows."[218] Since such a concept of protection leaving the specification of the purpose to the controller's will serve a "glaring loophole",[219] Nissenbaum comes to the conclusion that another concept focusing on a principle for "respect for context" is "something materially different, something better."[220]

In essence, Nissenbaum's criticism of the principle of purpose limitation refers to the same challenges as mentioned in the introduction of this thesis. However, considering a context-based approach as materially different and (sic!) better than a purpose-based approach requires, at first, determining the "tertium comparationis" (i.e. the commonality allowing a

---

216 See Nissenbaum, p. 134 referring to Schatzki, T (2001), Practice Minded Orders, in: The Practice Turn in Contemporary Theory, ed. T. R. Schatzki, K. K. Cetina, and E. von Savigny, London: Routledge, pp. 42 to 55.

217 See Nissenbaum, Respect for Context as a Benchmark, p. 291.

218 See Nissenbaum, ibid., p. 292.

219 See Nissenbaum, ibid., p. 291, referring to Fred Cate (2006), "The failure of Fair Practice Information Principles," Consumer Protection in the Age of the Information Economy, July 8. Accessed July 1, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

220 See Nissenbaum, ibid., p. 292.

comparison) of both approaches.[221] In addition, such a conclusion presupposes that there is no framework for helping to determine, similar to the approach of contextual integrity, substantive criteria for the specification of the purpose. Such an implicit presumption is particularly important for Nissenbaum's conclusion, since she admits that the success of her approach also depends on how the "context" is interpreted.[222] However, her observation that the principle of purpose limitation constitutes, without such a framework providing for substantive criteria, a mere shell remains valid. In 1989, the German legal scholar Badura equally criticized the legislation process of the German Federal Data Protection Law and at the time stated that it remained unclear "what the term 'purpose' actually means (…)".[223] However, the term "context", with respect to its function to a right to privacy, today is clearer in particular in light of Nissenbaum's approach. Thus, it should be possible to elaborate on a concept that equally clarifies the term "purpose". Indeed, before turning to this task it is necessary to clarify the interrelationship between both terms "context" and "purpose" because legal scholars, as well as data protection authorities, often use these terms 'simultaneously, at least, without explicitly clarifying the precise differences in their meaning.[224]

In its "Decision on Population Census", the German Constitutional Court provided the first and, compared to its following decisions, most comprehensive approach in defining both terms and explaining their interrelated functions. In order to determine the extent of the basic right to informational self-determination, it held that "it is not only necessary to examine the type of the data provided but also to examine the possibilities of

221 Cf. Bygrave, p. 157, associating the criteria of „context" with „purpose compatibility" and also the individual's „reasonable expectations" (with respect to this latter relationship, see in particular below under C. II. 1. a) ECtHR and ECJ: Almost no criteria.

222 See Nissenbaum, ibid., p. 292.

223 See Albers, Treatment of Personal Information and Data, cip. 124 quoting Peter Badura, Anhörungsbeitrag in der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages vom 19. Juni 1989, in: Deutscher Bundestag (Hrsg.), Fortentwicklung der Datenverarbeitung und des Datenschutzes, Zur Sache 17/1990, S. 15 (16): "Es sei unklar, was denn Zweck überhaupt ist, wie eng oder wie weit der Zweck zu sehen ist, ob Zweck etwa gleich Aufgabe ist oder organisatorisch definiert werden kann usw."

224 See, instead of many, the Article 29 Data Protection Working Grouop, Opinion 03/2013 on purpose limitation, pp. 23 and 24.

its usage. *These depend, on the one hand, on the purpose of the collection and, on the other hand, on* the possibilities of the specific technique of processing the data and on the possibilities of its combination. Consequently, a datum that is, per se, irrelevant can become relevant; insofar, under the conditions of automated data processing, there is no 'irrelevant' data. Whether information is sensitive cannot only depend on the intimacy of the events. In order to determine the relevance of the datum for the personality right, it is rather necessary to know *the context of its usage*. Only when it is clear for which purpose the information is required and which possibilities of linking and usage exist, it is possible to answer the question of whether the infringement of the right to informational self-determination is constitutionally legal or not (underlining by the author)."[225] In essence, the Court clarified that the relevance of data with respect to the personality right of the data subject does not only depend, similar to Nissenbaum's approach, on the type of data or the intimacy of the event, but also on further factors.

One decisive factor for determining the legal relevance of data is, from the Court's perspective, the context of its usage. Interestingly, the Court determines the context by referring to the purpose of the collection of the data, as well as referring to the actual technical possibilities of how the data can be combined and used.[226] Therefore, in order to answer the question of what the term purpose really means, it seems plausible to refer to contexts in the meaning that Nissenbaum describes. The specification of the

225 See BVerfG, 15th of December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83, cip. 176 and 177: "(...) Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr. Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten. (...)"

226 See also Britz, Informational Self-Determination between Legal Doctrine and Constitutional Case Law, p. 575.

purpose serves, from this perspective, to pre-determine the (future) context of the intended use of data and, thus, the context-related informational norms. Indeed, Hofmann already stated in his work *Purpose Limitation as Anchor Point for a Procedural Approach in Data Protection* from 1991 that the specification of the purpose serves to create "well-designed, transparent and controllable structures" and its limitation to "maintain the original context of collection".[227] Pohle stresses the similarity, if not equality, of these functions with Nissenbaum's approach of "contextual integrity".[228] In any event, the determination of a future context in advance through the specification of the purpose makes it possible to determine, for example, the transmission principles before the use of data takes actually place. Having the considerations on the regulation of risks in mind, referring to the purpose of the data processing enables the data controller to apply the transmission principles (or to prepare their application) in advance in order to avoid the (potential) later harm, that means, a later violation of contextual integrity. So far, the requirement to specify the purpose would not be a mere shell as Nissenbaum promotes. Instead, it is just another legal link for regulation. This approach focuses, by expanding legal protection before the violation of contextual integrity can take place, on the prevention of or precaution against risks for the individual's autonomy.

However, despite the German Constitutional Court's elaborated approach, the difference between both terms "context" and "purpose" is not sufficiently clear when reviewing the different acts of data treatment, i.e. stages of the information flow: Firstly, there is no clear distinction between contexts of different acts of data treatment over time. The Court only refers to the context of later usage. In contrast, the collection of data is also embedded in a certain context. This differentiation is important in order to exactly determine, as Nissenbaum proposes, the context in which the data usage precisely occurs and whether this use challenges the corresponding informational norms or not. Furthermore, the difference is im-

227 See Hofmann, Purpose Limitation as Anchor Point for a Procedural Approach in Data Protection, p. 25/26 regarding the first quote, and p. 126 regarding the second quote; cf. Bygrave, Data Privacy Law, p. 153, who highlights the importance of the principle of purpose limitation "ensuring adequate information quality and that the data-processing outcomes conform with the expectations of data controllers".

228 See Pohle, Purpose limitation revisited, footnote 24, referring to Helen Nissenbaum, Privacy as contextual integrity, Washington Law Review 79, pp. 101 to 139.

portant in order to obtain a clear distinction between the purpose specified the moment the data is collected and each later use of data. The reason is that one must be clear about the fact that each time the data is used, this use might pursue another purpose which would then determine another future context of the data treatment etc. etc. The second unclear aspect is that there is no specific explanation for the interplay between, *the purpose of the collection and (...) the possibilities of the specific technique of processing the data and on the possibilities of its combination*. The Court thus differs between the usage intended by the data controller and the usages that are factually possible. In doing so, the Court appears to imply that all factual possibilities of data processing could be pre-determined. Such an implication becomes reasonable in light of the data processing techniques that had existed at the time. In the 1980's, data processing was based on very few large central-computing systems. These central systems determined the different phases and possibilities of the processing of data and its possible combination. The legal terms of *collection, storage, processing, change, usage, and deletion of personal data* actually followed the technical environment at the time. Instead, today, the treatment of personal data often takes place in highly decentralized and non-linear environments. The different stages of the treatment of data, such as the collection, changing, combination, and transfer of data – how it is often described in literature and within the German law – do not necessarily succeed in this linear direction. Instead, in today's non-linear environment, these different types of data processing occur simultaneously or parallel and are intertwined, again and again, with the information constantly retrieved. Consequently, the information depends, more than before, on the corresponding context of usage.[229] This leads to the result that the computing system as such cannot determine all factual possibilities of data processing. A concept protecting (in other words, preserving) principles of privacy and/or data protection and, thus, a definition of the terms "context" and "purpose" must mirror this consequence.

In conclusion, in light of the fact that de-centralized and non-linear environments do not allow for the pre-determination of all factual possibilities of data processing, one has to, firstly, focus on examining the present

229 See Albers, ibid., cip. 121 and 122; highlighting the current change of the computational systems and environments compared to the times of the first "*Decision on Population Census*" in 1983, Hoffmann-Riem, Protection of the Confidentiality and Integrity of Information Technological Systems, pp., 1009 and 1010.

context in which the data is currently processed. Secondly, an appropriate legal link for determining the future context, is the present purpose. Therefore, in this thesis, the term "purpose" means the intended reason behind the data controller's treatment of the data referring to a future context; from this point of view, the realization of the purpose is a causal process with, at least an analytical final end that is determined by this purpose. The purpose serves to bundle the different acts of the data processing to a meaningful unity. From the perspective of the entity setting the purpose, the purpose thus decides on whether the means, which are used in order to reach the purpose, are appropriate or not.[230] In contrast, the term "context" does not primarily refer, be it a present or future one, to a certain result of a human-caused process but, as quoted previously, to "structured social settings with characteristics that have evolved over time (sometimes long periods of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more."[231]

So far, this definition of the term "purpose" does not exclude or substitute the "context" as defined within the framework of contextual integrity but rather incorporates it. Indeed, Nissenbaum also refers, in turn, to the term "purpose" when she elaborates on the definition of context. However, it is obvious that her context definition referring to the 'causes and contingencies of purpose' rather means the value, objective or end of a specific context than the subjective purpose formulated by an individual within that context. In any event, this thesis explicitly ties into the definition by the German Constitutional Court considering a purpose set by an individual not only referring to a future context of the data use, but also as another factor characterizing the present context. The reason is that a determination of the legal responsibility of the entity processing personal data, must also take its purpose into account. Without the knowledge about the purpose of the processing, it would be hard to determine the reason of the entrepreneurs behavior and, thus, at least, the entrepreneurs social role.[232] Hence, the context of a data treatment includes the purpose of the data processing – and this purpose characterizes, together with further circum-

230 See Albers, ibid., cip. 123; Pohle, Purpose limitation revisited, pp. 142 and 143; see, from a sociological perspective, Luhmann, The Concept of Purpose and the Rationality of Systems, in particular, pp. 1 ff., 9 ff. and 114 ff.

231 See Nissenbaum, ibid., p. 130.

232 Cf. Nissenbaum herself with respect to the necessity of knowing the purpose of a context in order to understand it, ibid., p. 134.

stances, the corresponding context. A purpose thus links the existent context of the current act of data treatment to a future, intended one.[233]

By means of an example: The startups mentioned in the introduction each publish their own websites, in order to improve the process and experience of users of their websites, and use the service of a provider of analytical tools, who in turn analyze the behavior of the users visiting the website. This analysis is based on the collection and processing of user data, such as the time and date of his or her visits, the visit behavior (for example, from which page does the user come from, on which page does he or she start, how much time does the user stay and when does he or she leave) as well as, possibly, the user's IP address, the location and type of his or her device and the browser ("attributes"). The moment a user's data is collected, the context is determined by: the publisher of the website using the service of the service provider, the service provider itself (both with respect to their corresponding purposes) and the social role of the data subject the moment when he or she uses the website ("actors"); the general expectations of whether the data might be collected or under which conditions and for which purposes it might be used ("norms"). Thus, the purposes of the website publisher and the service provider determine, amongst others, the context of the data collection. The future contexts can be, given that the website publisher and the service provider constantly develop their products further, mainly prescribed by these purposes. The way the website is developed and the analytical software used per se, only allows in a limited way to pre-determine, pursuant to the technical environment, the future context of the concrete data processing.

5. Values as a normative scale in order to determine the "contexts" and "purposes"

However, this example evidences that there is, over time, not only an unlimited number of contexts in which the data processing may occur but also, an unlimited number of purposes which pre-determine these contexts. Accordingly, the service provider collects the data, deletes certain other data and combines it with further data, firstly, for the purpose of analyzing it. The analysis as such takes place for the purpose of transferring

233 Cf. Albers, ibid., cip. 121 and 122.

the analytical results to the website publisher and, possibly, in order to improve the functioning of its analytical software. While all purposes take place in order to maintain the corresponding businesses, the service provider may know or not know the true purposes of the website publisher using the analytical results. The publisher of the website might use them, as described above, for the purpose of improving the user experience of its website but also in order to present it to (potential) cooperation partners and financiers. Even the storage of the data for an unknown purpose is, as such, a purpose. Hence, there are many acts of a data treatment occurring iteratively or simultaneously for many different purposes and, consequently, in corresponding contexts. For example, the purpose of a preceding act can lead to a following one, i.e. a subsequent purpose, or be completely different. Depending on the respective purposes, data may not only be intended to be transferred from one context into another one, but also the context in which the processing occurs may remain the same or turn into another one. The reason for this change is that the determination of the context depends on the perspective of the observer (whoever exercises this judgment task), just like the specification of the purpose depends on the actors' point of view. The question therefore is how to distinguish the different purposes and contexts, as well as the different acts of data treatment from a legal point of view: Which acts of the data treatment, which corresponding purposes, which contexts are legally relevant?

Nissenbaum herself provides a solution to this question: The values serve as the main criteria for determining a context as a common unity of analysis. Values explain the reason of behavior in a context and, thus, which elements observed are relevant within this context and which are not. Values hence not only help answer the question of which new informational norms that challenge entrenched ones are justified, but already, in a preceding step, the question of how to determine the specific context, i.e. which elements observed belong to a specific context and which not. As a consequence, values may fulfill the same function in order to determine the relevance of the purpose of data processing. From this perspective, the main task of this thesis is then to elaborate on such values as a normative concept that can assist in determining context-relative informational norms and, in this framework, the function of the principle of pur-

pose limitation.[234] This may imply answers to the question of how precisely purposes of data processing must or how broadly they may be specified.

234 Cf. De Hert and Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, p. 4, summarizing how data protection regulation "formulates the conditions under which processing is legitimate."