A. Introduction

Dating back to the early discussions regarding the concept of data protection, the so-called "principle of purpose limitation" is one of the fundamental principles of data protection law.[1] The principle essentially requires that personal data may only be processed for the original purpose of collection of the data,[2] or in the words of the OECD Privacy Guidelines, at least, so long as it is not incompatible with the original purpose.[3] In light of our ever increasing digitization of society, the principle of purpose limitation is more and more debated amongst legal scholars.[4] The most recent motivations behind these discussions arose because the European Council's draft of the General Data Protection Regulation was leaked in the beginning of 2015 by the non-profit association European Digital Rights (EDRi).[5] Article 6 sect. 4 of the European Council's draft widely abandoned the principle of purpose limitation by stating that personal data can be used, even if it is incompatible with its original purpose, so long as it can be based on a legal provision in accordance with Article 6 sec 1 lit a-e. An exception to this rule is Article 6 sect. 1 lit. f of the draft, which provides that the collection of data is legal if it is "necessary for the purposes of the *legitimate interests* pursued by the controller (underlining by the author)". Only if the collection of personal data is based on this provision,

1 See Article 29 Data Protection Working Group, Opinion 03/0213 on purpose limitation, pp. 4 and 6 ff.; Handbook on European data protection law, p. 68; De Hert and Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, p. 4; Bygrave, Data Privacy Law, p. 153; v. Zezschwitz, Concept of Normative Purpose Limitation, cip. 1; Pohle, Purpose limitation revisited, p. 141; contrary, Härting, Purpose limitation and change of purpose in data protection law, who affirms the requirement of purpose limitation only applicable to the legislator but not to the data controller.

2 Cf. v. Zezschwitz, Concept of Normative Purpose Limitation, cip. 14.

3 See no. 9 of part two of the OECD Privacy Framework, p. 14.

4 See, instead of many, Cate/Cullon/Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century, p. 11.

5 See the documents linked by Naranjo, Leaked documents: European data protection reform is badly broken, retrieved on the 2nd of February 2016 from https://edri.org/broken_badly/.

then the principle of purpose limitation should apply.[6] European Digital Rights particularly criticized this extensive abandonment of the principle of purpose limitation because it would undermine "control and predictability" as "the core of data protection".[7] In essence, this doctoral thesis addresses the question of whether this consideration is true or not, or from a more academic point of view, what the function of the principle of purpose limitation actually is.

I. Problem: Conflict between innovation and risk protection

From an academic perspective, there are two main aspects of the principle of purpose limitation that are particularly interesting: Firstly, the principle of purpose limitation appears to conflict with the societal needs for innovation and is the perfect example of a more general conflict for the regulators: How can the legislator enable or enhance innovation and, simultaneously, protect against its risks? The second aspect refers to the uncertainty of how to apply the principle of purpose limitation in general. Only if the principle of purpose limitation was clear and we knew what is actually meant, would it be possible to answer the preceding question.

1. Innovation as an economic driver for public welfare

A multitude of international studies and policy recommendations brings the importance of innovation for the public welfare more and more into public debate. For instance, the OECD Science, Technology and Industry Outlook 2014 considers: "Innovation is a major driver of productivity and economic growth and is seen as a key way to create new business values."[8] Another OECD report focusing on data-driven innovation considers its positive effects as "significantly accelerating research and the development of new products, processes, organisational methods and markets".[9]

---

6 See Grafenstein, The Principle of Purpose Limitation between Openness toward Innovation and the Rule of Law, DuD 2015 (12), p.789.
7 See EDRi / access / Privacy International / Fundacja Panoptykon: Data Protection Broken Badly.
8 See OECD Science, Technology and Industry Outlook 2014, p. 21.
9 See OECD: Data-Driven Innovation for Growth and Well-Being.

The World Economic Forum draws, in its 2014 report on how to enhance Europe's competitiveness, the attention to entrepreneurship as the key source of innovation.[10] From an entrepreneurial perspective, however, the law is usually not perceived as a driver of but rather barrier for innovation. The Eurobarometer on "Entrepreneurship in the EU and beyond" surveyed that a "large majority of respondents (..) agreed that business start-ups were difficult due to complex administrative procedures: 71%, in total agreed and 29% strongly agreed."[11] Similarly, the Global Entrepreneurship Monitor 2014 surveyed, amongst others, "the lowest evaluation corresponded to government policies toward regulation".[12]

2. Protection against the risks of innovation

This perception corresponds to the general view amongst innovation researchers who consider that the law actually acts as a barrier rather than as a pro-active instrument which would influence and develop, besides other factors, the process of innovation. The reason for this perception might be that the term "innovation" usually refers to something unexpected and new, while the law seeks to guarantee a certain and expected outcome.[13] The principle of purpose limitation restraining the later use of personal data to the original purpose of collection indeed appears to be diametrically opposed to such unexpected outcomes of innovation. However, the public discussion also recognizes the risks caused by innovation. The abovementioned OECD report not only considers the positive effects of data-driven innovation but also its risks, in particular, for privacy and security.[14] Having applied a "bottom-up cultural analysis of historical, philosophical, political, sociological, and legal sources", Solove elaborated in his book *Understanding Privacy* on a taxonomy of 16 privacy risks and/or harms, from the collection of information to its processing and distribution as well as invasion.[15] In this regard, two terminological issues shall briefly

10 See World Economic Forum: Insight Report: Enhancing Europe's Competitiveness – Fostering Innovation-Driven Entrepreneurship in Europe.
11 See Eurobarometer: Entrepreneurship in the EU and beyond, p. 75.
12 See Singer et al., Global Entrepreneurship Monitor – 2014 Global Report, p. 14.
13 See Eifert, Innovation-enhancing Regulation, p. 11 and 12; cf. also Lipshaw, Why the Law of Entrepreneurship Barely Matters.
14 See OECD: Data-Driven Innovation for Growth and Well-Being.
15 Solove, Understanding Privacy, pp. 101 ff. as well as 171 ff.

be clarified: so far, this thesis does not (yet) differentiate between the terms *data* and *information*;[16] second, except of this differentiation, this doctoral thesis does not make a difference between the terms "processing", "treatment", "use" and "usage" of data and/or information. In any case, the study "Commercial Digital Surveillance in Daily Life" summarizes the most common or, at least, commonly known cases of *data mining techniques* (for example, predictive analytics about one's pregnancy, status of relationship or emotional state of mind based on purchase behavior, Facebook likes or keyboard usage patterns) and its commercial exploitation in the insurance, finance or HR industry.[17] Boyd and Crawford stress in particular the high subjectivity and potential inaccuracy of those data mining techniques.[18] The regulator must thus not only seek to enable and enhance innovation but also to protect against the risks caused by innovation.[19] In conclusion, the question therefore is which role the principle of purpose limitation plays within this regulatory conflict between enhancing innovation and protecting individuals against its risks.

3. Uncertainty about the meaning and extent of the principle of purpose limitation

This leads to the second reason that makes an academic examination of the principle of purpose limitation interesting: the uncertainty about its precise meaning and extent. In order to apply the principle of purpose limitation, it is necessary to determine the original purpose of collection. The main question hence is how precisely the original purpose must or, vice versa, how broadly it can be specified: the wider that the original purpose is specified, for example, the purpose of money making, the broader the scope of action will be for the controller and/or others to be able to use that data for the same purpose.[20] However, the question how precisiely a

16 See the differentiation below under point C. I. 3. c) cc) (1) "The reason for why the scope is too vague: Difference between data and information".
17 See Christl, Commercial Digital Surveillance in Daily Life.
18 Boyd and Crawford, Critical Questions for Big Data, pp. 666 ff.
19 See Hoffmann-Riem, Innovation Responsibility, p. 16.
20 See Forgó et al., Purpose Specification and Informational Separation of Powers, p. 34; Mehde, Handbook of European Fundamental Rights, cip. 24; in contrast, see Bygrave, Data Privacy Law, p. 155, who considers this first component of the principle of purpose limitation "relatively free of ambiguity".

processing purpose must be specified is an open question. Comparably, regarding the second component of the principle of purpose limitation, i.e. the question of under which conditions another (later) purpose is compatible with the original purpose, there are only few reliable criteria, if at all, that help really answer this question. The Article 29 Data Protection Working Party refers in its "Opinion 03/2013 on purpose limitation" to a bundle of criteria (see, now, also Art. 6 sect. 4 GDPR) such as the relationship between the original purpose and the further processing, the context of collection, the nature of the data and the impact caused by the later use on the individual, as well as the safeguards applied in order to prevent any undue impact.[21] However, these criteria also pose two problems: First, each criteria lacks an objective scale which would help to determine, for instance, the "relationship" between the purposes; and second, the fact that all criteria together can be used as an entire basis to reach a decision, produces different results amongst decision makers who weigh the criteria against each other. Interestingly, there is little academic literature on the precise meaning and extent of the principle purpose limitation that allows one, in light of the fundamental rights concerned, to determine reliable criteria.[22] This is particularly the case since most of the publications refer to the processing of personal data by the State, and not in the private sector, which is what this thesis focuses on.

4. Practical examples referring to two typical scenarios

Both aspects, i.e. the appearing conflict of the principle of purpose limitation together with the openness of innovation processes, and the ever increasing uncertainty about how to apply this principle within our current technological environment, result from the ambiguity of the current legal concept of protection. The following examples shall give the reader of this thesis an impression of the effects of this ambiguity in today's business world.

---

21 See Opinion 03/2013 on purpose limitation, pp. 23 to 27.

22 See only Hofmann, Purpose Limitation as Anchor Point for a Procedural Approach in Data Protection; Forgó et al., Purpose Specification and Informational Separation of Powers; Eifert, Purpose Compatibility instead of Purpose Limitation; Albers, Treatment of Personal Information and Data, cip. 123.

a) Coming from a practical observation: Startups and non-linear innovation processes

Practically, for the past three years, I have often discussed this issue with founders of Internet-enabled startups in the *Startup Law Clinic* of the *Alexander von Humboldt Institute for Internet and Society* (HIIG), and the specific legal challenges they face in trying to develop and implement their business model in today's society.[23] The *Startup Law Clinic* is part of the interdisciplinary research project *Innovation and Entrepreneurship.*[24] Based on empirical data gathered in these Startup Clinics, the research project aims to understand, on a more efficient level, Internet-enabled entrepreneurship. In doing so, the project focuses on Internet-enabled startups that are, pursuant to some business observers "turning the conventional wisdom about entrepreneurship on its head."[25] For instance, Blank observes that startups differ to traditional larger companies, amongst other aspects, in how they react or adapt to uncertainties: While traditional companies create long-term business plans based on the "assumption (..) that it's possible to figure out most of the unknowns of a business in advance" and then execute such plans, step-by-step, according to the so-called waterfall principle, "lean" startups *search* for a business model going "quickly from failure to failure, all the while adapting, iterating on, and improving their initial ideas as they continually learn from customers."[26] Such a methodological difference does not mean that traditional larger companies are not able to apply the same methods as startups do. In contrast, authors like Blank, as well as Ries, argue that traditional companies more and more apply this methodology.[27] However, startups are known to apply this methodology most rigorously in light of the particular uncertainty they face. Ries, at least, defines a startup, amongst others, as being "designed to confront situations of extreme uncertainty."[28] Unlike a "clone of an existing business", an innovative startup is always looking for "novel scientific

23 See the preliminary findings in the Working Paper by Dopfer et al., Supporting and Hindering Factors for Internet-Enabled Startups, pp. 23.

24 See the description of the research project retrieved on the 4th of February 2016 from: http://www.hiig.de/en/project/innovation-and-entrepreneurship/

25 See Blank, Why the Lean Start-Up Changes Everything; cf. also Blank, Four Steps to the Epiphany, as well as Ries, The Lean Startup.

26 See Blank, ibid.

27 See Blank, ibid.; Ries, ibid, pp. 36 and 37.

28 See Ries, ibid., p. 38.

discoveries, repurposing an existing technology for a new use, devising a new business model that unlocks value that was hidden, or simply bringing a product or service to a new location or a previously underserved set of customers" and, thus, confronted with constant change.[29] Indeed, this phenomenon also became apparent in the *Startup Law Clinic*.[30] Therefore, with respect to startups developing their business models based on the processing of personal data, it was interesting to figure out how far they were, in effect, able to apply the principle of purpose limitation. Not surprisingly, there essentially were two types of cases particularly relevant when seeking to find an answer to this question: The first case refers to situations where startups want to process data of its own users but cannot yet specify the purpose of the later processing; the second case concerns situations where startups want to process personal data that was originally collected by a third party. In this second case, the problem for the startups was not only their own inability to specify the new purposes, but also the high uncertainty about the precise meaning and extent of the legal requirement to restrict their processing to the purposes initially specified by the third party when the data was first collected.

b) First scenario: Purpose specification by the controller concerning the use of data of its users

In the first case, the main problem exists in the controller's limitations to specify the purpose of collection. The main reason for this limitation is the openness of its entrepreneurial process. The following example shall illustrate this process and the resulting problem with respect to the requirement of purpose specification.

aa) The unpredictable outcome of entrepreneurial processes

One startup, which exemplifies this conceptual issue, was started in early 2014 with the idea to develop a wallpaper app for smartphones with android operating systems. Android operating systems allow the user (and their apps) to interact on the home screen of the smartphone with the un-

29 See Ries, ibid., p. 38.
30 Cf. Dopfer et al., Supporting and hindering factors for internet-enabled startups.

derlying interface. In essence, the mobile app enabled its user to choose different background pictures (via a double tap on the home screen), to zoom into certain parts of the picture, to fade out to full screen, to like and to share it. The pictures were tagged with certain categories such as "red" for the main colour or "car" for the theme so that they could be matched with profiles of the users.

The startup wanted to create these profiles in order to deliver image advertising pursuant to the users' usage behavior. The startup's business model consisted in the revenues received from its advertising partners paying for the personalized advertising space. So far, this purpose, the collection of personal data for advertising as explained before, and the way of how this data was processed, could easily be specified before the start of the closed beta test using 20 users. Indeed, as a result of the closed beta test, the startup decided in the middle of 2014, to broaden its concept: Instead of a pure wallpaper app, the app should become a new media format enabling its users to explore different kinds of media. The wallpaper picture should serve as the visual entry point for the user to follow, still via the double tap on the home screen, a link to the actual media format such as the new album of a music band, the newspaper article or, still, the image advertising. Even if this concept was still based on the profiles of the app users, the business model has now changed. Now, not only advertisers should pay for advertising space, but also additional business partners, such as newspapers and music editing houses, should pay the startup a percentage of the price received for selling their online offers to the app users. Hence, the question was whether or not the original purpose still covered the new purpose and the processing operations. Taking into account possibly later changes, the startup had, in the first *Startup Law Clinic* session, before the closed beta test, used an umbrella: Before the startup specifically described the concrete purpose, data and means of the processing, it had clarified that the whole processing pursues the purpose of "personalized marketing". However, the Article 29 Data Protection Working Group stated in its "Opinion 03/2013 on the principle of purpose limitation" that the term of "marketing purposes" would be too broad.[31]

In the course of the following months, the startup started an open beta test for its app, which quickly got up to 30.000 users, and therefore looked

31 See Article 29 Data Protection Working Group, Opinion 03/0213 on purpose limitation, p. 16.

for further private investors. However, the search for a working business model remained very difficult. In April 2015, the startup joined, having now around 100.000 users, a round table discussion with finance experts organized by the *HIIG Business Model Innovation Clinic*. On this occasion, one founder of the startup gave a short presentation, in particular, about the success regarding the user growth and the on-going struggle to find a functioning business model. After a brief discussion, one finance expert provided a solution for the problem: Why spend so many efforts on finding the business model if the user growth was still exploding? The experts' advice was simply to focus, so far, on the user growth. The expert continued to advise and stated that as soon as the number of users was large enough, the startup would only then find out which revenue model would work later on. Equipped with such advice, indeed, the startup was not able to definitely specify the purpose of its later use of the collected data. Even the broad purpose of "personalized marketing" was just a guess. In beginning 2016, the startup had 180.000 users and was still looking for the business model.

bb) Excursus: In which circumstances do data controllers actually need "old" data?

This example of an iterative development process for a mobile app illustrates how difficult it may become, if not impossible, to specify the purpose of all-later processing operations when the data is collected. However, data-driven innovation does not require, in general, that the entrepreneur must be able to use all personal data that has ever been collected. In contrast, for many innovations, it may be sufficient to use data that was only recently collected: If the qualitative data gathered by the startup is just good enough or the user base just large enough, the startup might be able to find its business model or even deliver personalized marketing on an "almost-real time" basis. In conclusion, even if an iterative process principally hinders entrepreneurs to specify the purpose of a later processing, this must not necessarily be so in each particular case.

c) Second scenario: The limitation of the later use of data collected by third parties

As mentioned previously, the second constellation refers to controllers processing personal data that another entity collected originally. In these cases, the problem is not only the iterative entrepreneurial process itself which hinders the controller to specify the purpose of the later processing. Rather, the purpose originally specified by another entity might hinder the controller in its entrepreneurial process. Indeed, it is characteristic for a law to hinder someone's action in order to protect another one.[32] However, the essential point here is to illustrate the uncertainty accompanying entrepreneurial activity when controllers seek to apply the principle of purpose limitation. Two further examples shall illustrate this conceptual uncertainty.

aa) No foreseeable negative impact on individuals

The first example is about a startup that retrieved personal data from social network communities such as Facebook and Twitter via a public API, in order to create so-called *social heat maps*. The social heat map was designed to predict not only the places, but also how many people would be and at what time and for what reason at a certain establishment. One economic business idea of the startup was to sell this information to taxi drivers enabling them to plan their driving routes in a more efficient manner. In order to achieve this objective, the startup transferred data from the social networks' servers to their own servers. The transferred datasets contained data that related to geo-locations of events organized by users via the networks, as well as of users themselves sending a signal from where they were (so-called check-ins). The moment that the data was transferred to the startup's own servers, a self-learning algorithm sorted out the specific data which was useful in order create the social heat map. So far, the participants of the *Startup Law Clinic* sessions, could not see a negative impact on the users' concerned. Indeed, it was the opposite. The participants could only actually see a positive effect in that the users, possibly, will more likely find a taxi, for example, when they come out of a concert

32 Cf. Hoffmann-Riem, Openness toward Innovation and Responsibility for Innovation by means of Law, p. 258.

or a restaurant. The participants particularly came to this conclusion because the startup anonymized the data the moment it had retrieved it from the social networks (via the public API). However, with respect to the current data protection framework, the problem was that the data was not made anonymous before its retrieval. This lead to directive 95/46/EC (Data Protection Directive) being applicable, in principle.[33] As a consequence, two legal issues arose.

The first issue concerned the legitimate basis of the data processing intended by the startup. Social networks usually base their processing of data on their users consent. However, the consent given produced two problems. On the one hand, the consent may not cover the later use of the data intended by the startup, because the social network could not foresee the later usage. On the other hand, the purpose may be specified as being so broad that it ran the risk of not being sufficiently precise (e.g. the purpose of 'transfer to third parties'). Therefore, the startup had either to base its data processing on an additional consent given by the users concerned, or on another legitimate basis provided for by law, (as stipulated in Art. 7 of the Data Protection Directive, as well as in Article 6 of the General Data Protection Regulation). Since the startup would have had, in light of the amount of data concerned, practical difficulties to get the consent of all users' concerned, the startup focused on another legitimate basis provided for by law. Indeed, whether this 'secondary option', i.e. referring to a legal provision when the individual's consent does not cover the intended processing, would have been legal was also questionable because it might be seen as a circumvention of the original consent.[34] In any event, even if this had been possible, it was unclear whether or not the startup could base the data processing on, in particular, the general clause of Article 7 lit. f of the Data Protection Directive (correspondingly, Article 6 sect. 1 lit. f of the

33 The directive itself was, indeed, not directly applicable since it must be transposed into national law in order to directly bind the data controller; for the sake of simplicity, however, this thesis does refer, so far, to the directive and not national law; with respect to the transposition into national German law, see, in more detail, point C. II. 1. c) "Transposition of the requirement of purpose specification into German law".

34 Cf. Gola/Schomerus, Federal Data Protection Law, § 4 cip. 16; in contrast, see Article 17 sect. 1 lit. b GDPR, which excludes the individual's right to require from the controler, based on an objection to his or her consent, to delete the personal data if the controller can base the processing on another legitimate ground foreseen by law.

General Data Protection Regulation). This Article allows the data processing if it "is necessary for the purposes of the legitimate interests pursued by the controller (…), except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject". Whether or not this provision covered the intended data processing was doubtful because the balancing exercise based on the bundle of criteria again produces legal uncertainty.

In the *Law Clinic* Session the participants examined the users consent and it became apparent that the original purpose was not identical with the later use intended by the startup or was not sufficiently precise. Therefore, the second question became additionally relevant: whether or not the later processing intended by the startup was in accordance with the compatibility assessment proposed by the Article 29 Data Protection Working Party with respect to Article 6 sect. 1 lit. b of the Data Protection Directive (correspondingly, Article 5 sect. 1 lit. b of the General Data Protection Regulation).[35] On the one hand, there was no negative impact on the individuals concerned; it seemed to be the same context (communicating with friends and going to social events = private/leisure life?); and the data was, once retrieved by the startup, immediately anonymized. On the other hand, the relationship between the original purpose of collection (connecting friends) with the later processing by the startup (creating social heat maps) was disconnected; the data was sensitive (geo-location data)[36]; and the users of the social networks did not probably expect this kind of usage. Hence, even if there was no intended negative impact on the users of the social networks concerned and the data was immediately anonymized, there was enough legitimate criteria resulting in the finding that the later use was incompatible with the original purpose of collection.

bb) Negative impact foreseeable on the individuals

In the second example, the participants of the *Startup Law Clinic* session could clearly target a possible impact on the individuals concerned by the

35 See the Art. 29 Data Protection Working Party, Opinion 03/2013 on the principle of purpose limitation, pp. 20 ff.

36 Cf. the Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC, p. 38.

data processing. A startup retrieved generally accessible personal data from professional networks. The startup created, in a first version, profiles based on the data that users of the professional networks have made publically available. The profiles contained predictions about three characteristics of the users of the professional networks that could potentially interest future employers: First, the probability that the user changes his or her current employment; second, the probability that the user would also change the city for a new employment; and third, the degree of expertise in a certain professional domain or area. The startup sought to sell the access to these profiles to the human resources departments of companies in the private market as the access to the profiles, would enable the human resources departments to make better decisions when finding and/or considering the right candidate for a certain job. Since the employer was intended to connect the profile with the candidate, the data could not be considered anonymous. Additionally, in light of the fact that the focus was to sell the product to employers, only, the potential employees (i.e. the users of the professional networks) would not be able to gain access to the database as a whole or to their specific profiles. Similar to the preceding example, two main questions arose.

First, whether or not the later use of the personal data could be based on the users' consent or another legitimate basis provided for by law. Here again, the consent sought by the professional networks from its users did not either cover the later use or was too broad in its purpose. Hence, the startup had to base its data processing either on Article 7 lit. b or f of the Data Protection Directive (correspondingly, Article 6 sect. 1 lit. b or f of the General Data Protection Regulation). The first provision allows the processing if it "is necessary (…) in order to take steps *at the request of the data subject* prior to entering into a contract (underlining by the author)". In the example, the creation of the profiles and the access to it could hence only be necessary for the potential employer if the employee takes the initiative of actually applying for a job. For other cases where the employer searches for new potential employees based on their own initiative, only the general clause under Article 7 lit. f of the Data Protection Directive (and Article 6 sect. 1 lit. f of the General Data Protection Directive, correspondingly) came into question. Insofar, the participants of the *Start-up Law Clinic* considered the search (and help) for potential employees indeed was a legitimate interest. However, it was arguable whether or not the potential employee had an overriding interest, for example, for his or her freedom to choose an occupation protected under Article 15 ECFR.

This interest might have overridden the potential employer's (and the startup's) interest because of one particular reason. There was no reason for why the potential candidate could not be able to correct inaccurate data and add further advantageous information or do anything else which could improve his or her chances for being invited to the interview.

With respect to the compatibility of the purposes at hand, it was unclear whether or not the profiling of potential employees in order to find the right job applicants could be seen as a sub-category of the original purpose of the professional network to connect professionals and, thus, identical. In order to avoid any doubts, the participants of the *Law Clinic* session sought to apply the compatibility test proposed by the Article 29 Data Protection Working Party. The question of whether or not the later processing was compatible with the original purpose of the professional networks depended, indeed, on a bundle of criteria which was very similar, if not identical, to the balancing test required under Article 7 lit. f of the Data Protection Directive (and Article 6 sect. 1 lit. f of the General Data Protection Regulation).[37] There were several reasons in favour of the application: 1) the relationship between the later processing and the original purpose was close because the latter processing could have been considered as a sub-category of the first; 2) the data appeared not to be sensitive since it was published by the users and the categories of the profiles did not reveal any information about race, geo-location or similar information; 3) the later processing seemed to belong to the same context (professional life?); and 4) the user might consequently have expected the later use. On the other hand, the impact on the individual concerned could have been significant if he or she was filtered out, only for the reason that his or her profile did not match with the potential employer's expectations. This was even more the case if there was no official proof of whether or not the profile really mirrored the likeliness that the employee would not have the expected attributes.

37 Cf. the criteria proposed by the Article 29 Data Protection Working Group, Opinion 03/0213 on purpose limitation, p. 20 ff., and Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, pp. 33 ff.

5. Interim conclusion: Uncertainty about the concept of protection and its legal effects

In conclusion, albeit both of the two last examples significantly differed to each other with respect to the impact, it was hard, if not impossible, to answer the question if the later data processing was legal or not. Similarly, the first example already illustrated that the requirement to specify the purpose creates uncertainty in itself. This sheds light on what startups might mean when they express hope for improvement in political regulations and bureaucracy, rather than for social or advisory support.[38] However, it shall again be stressed that these examples should only *illustrate* the general questions of how to specify the purpose and determine which later use is compatible with the original purpose and which is not. An answer to these general questions does not depend on the practical examples but on the legal concept of protection. However, finding an answer to these questions is highly important for companies and organizations. These entities try to apply the law because of their reputation, amongst other factors.[39] If a data protection authority examines their use of data and comes to the conclusion that they are using that data illegally, there is a high risk of losing their reputation in the market. Consequently, the higher the risk of a loss of reputation, the more important it is for the processing entity to rely on clear criteria that would assist in correctly applying the law.

Correspondingly, the same uncertainty is true with respect to the individuals concerned by the processing of data. Hallinan and Friedewald examined in one of their works more than ten public opinion surveys supplemented by further sources such as ethnographic studies and focus groups regarding the European public perception on the data environment. One of their aims was to find out why individuals' behavior "at first sight appears erratic and even contradictory to declared privacy preferences."[40] Irrespec-

38 See Kollmann et al., European Startup Monitor 2015, pp. 62 and 63, indeed showing financial support as the even higher ranked hope.

39 Cf. Jarchow and Estermann, Big Data: Chances, Risks and Need for Action of the Swiss Confederation, pp. 14 and 15.

40 See Hallinan and Friedewald, Public Perception of the Data Environment and Information Transactions – A selected-survey analysis of the European public's views on the data environment and data transactions, pp. 62 and 76/77.

tive of differences in national perceptions,[41] the European public considers the protection of personal data as very important and that the disclosure of personal data raises significant concerns. However, individuals appear to accept the disclosure of personal data considering it as being "simply a part of modern life".[42] In order to explain the individual logic behind these contradictory observations, Hallinan and Friedewald referred to economic considerations proposed by Acquisti and Grossklags about potential limiting factors for rational decision-making.[43] In light of these considerations, the contradictions between general privacy awareness and specific disclosure of personal data result, in particular, from the following three aspects: First, individuals often only have a limited understanding of the risks implied in data transactions.[44] For example, while they are specifically aware of ID fraud as a serious threat, only few individuals consider or understand "the more abstract, invisible and complex aspects" such as "the value of the data, the nature of the technologies involved or the shape or nature of data flows – that is to say, (…) the critical parts of the data environment".[45] The second reason, besides limited information or conceptual understanding, is psychological distortion. Individuals tend, for instance, to prefer certain short-range rewards, such as an online service "for free", to uncertain long-range risks caused by a potential misuse of data. Finally, ideological or personal attitudes constitute another factor for why an individual might either not disclose personal data at all, albeit the benefits are higher than potential losses, or vice versa.[46]

Hallinan and Friedewald stress that these factors challenged the common understanding of economic behavior that the current data protection

41 See, for example, Vodafone Institute for Society and Communications: Big Data – A European Survey on the Opportunities and Risks of Data Analytics, p. 17, showing that "Germans are especially critical concerning privacy issues", while "South Europeans in the survey are generally more relaxed as far as the collection and use of their data is concerned".

42 See Hallinan and Friedewald, ibid., p. 65 and 68.

43 See Hallinan and Friedewald, ibid., pp. 70 et al. with reference to Acquisti, Alessandro and Grossklags, Jens, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in: Camp, J. L. and Lewis, S. (eds.), The Economics of Information Security, 2004 Kluwer, as well as ibid., "Privacy and rationality in individual decision making", IEEE Security and Privacy 2005, pp. 26 to 33.

44 See Hallinan and Friedewald, ibid., pp. 72 to 74.

45 See Hallinan and Friedewald, ibid., p. 75.

46 See Hallinan and Friedewald, ibid., p. 74.

system is actually built on. The misconception by the legislator about the individual's behavior might be the reason for why the European public has the feeling that the current laws do not fulfill their objective.[47] In light of this, critics recognize that current data protection law suffers, from both the individual's perspective and the controller's perspective, a "credibility crisis".[48]

Several legal scholars stress that this credibility crisis results from the uncertainty about the conception behind data protection law.[49] In particular, v. Lewinski unfolds, in detail, the different dimensions of protection covered by the broad term *"data protection*". While data protection laws are typically meant to regulate the relationship between individuals, on the one hand, and companies and the State, on the other hand, the object of protection, as well as the concept of protection is less clear.[50] In v. Lewinski's opinion, the term "data protection" refers to several objects of protection (i.e. the question of "what is protected") such as the individual's dignity, his or her private sphere, or the societal balance of informational power.[51] Similarly, there are several possible concepts of protection (i.e. referring to the question of "how to protect the objects") as: first, practical protection mechanisms such as self-protection; second, normative mechanisms such as social, technical and legal norms but also mechanisms of self-regulation such as standards, codes of conduct, and certificates; third, institutions that enable, for example, individual's self-protection, limit informational power, or enforce legal requirements; and fourth, the range of protection such as protection against concrete infringements, or specific risks and dangers, or even precautionary protection against unspecific risks and abstract dangers.[52]

47 See Hallinan and Friedewald, ibid., pp. 65 and 71.
48 See Kuner et al., The Data Protection Credibility Crisis, IDPL 2015 Vol. 5 no. 3, pp. 161.
49 Cf. Stentzel, The Fundamental Right to ...? The Search of the Object of Protection of Data Protection in the European Union, PinG 05.15, pp. 185; cf. Solove, Understanding Privacy; cf. v. Lewinski, The Matrix of Data Protection.
50 See v. Lewinski, ibid., pp. 1 to 16.
51 See v. Lewinski, ibid., pp. 7 as well as 17 to 63; see also De Hert and Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, p. 5.
52 See v. Lewinski, ibid., pp. 64 to 85.

Irrespective of whether or not this "matrix of data protection" is correct and comprehensive,[53] it does help clarify the question that the meaning and extent of the principle of purpose limitation cannot be answered without being clear on the object and concept of protection of data protection law. Only if the object and concept of protection are sufficiently precise, it is possible to answer the question of how to balance the need for innovation against its risks with respect to the processing of personal data.

II. Research questions and approach

Therefore, the research questions of this doctoral thesis are:

1. *What is the meaning and function of the principle of purpose limitation on the private sector, in light of the object and concept of protection of data protection law?*
2. *In order to find a balance between the societal need for data-driven innovation and protection against its risks, what regulation instruments should transpose the principle of purpose limitation in the private sector?*

In order to answer these questions, this doctoral thesis builds upon the research approach regarding innovation developed by the *Center of Law and Innovation* (CERI) in Hamburg, Germany.

1. Legal research about innovation

The CERI research project "Law and Innovation" reacted to the situation that at the beginning of 1990, legal scholarship had not yet started, at least not in Germany, doing research about innovation, in contrast to other research disciplines such as technical, economic, and social sciences.[54] Consequently, the object of this research approach does not primarily look to innovate the law, but rather how the regulator can regulate technological,

53 See v. Lewinski, ibid., pp. 87 to 90 commenting on the deficits of such a matrix and highlighting, however, its main use for structuring the public debate, enhancing legal comparison on an international level, and discovering deficits of legal protection.

54 See Hoffmann-Riem, Openness toward Innovation and Responsibility for Innovation by means of Law, p. 256.

economic and social innovation in today's society.[55] This approach acknowledges that the primary objective of the law is to protect against harm and risks and, thus, restricts the scope of action of entities that actual cause these harms and risks. Such a restriction, is in particular, at stake if the law expands its scope of protection from known risks to even unknown risks. One instrument for expanding the scope of protection, can be the so-called precautionary principle (as discussed in chapter B. II. Data protection as a risk regulation). However, regulating innovation, not only leads to the question of how to protect against the actual risks caused by innovation, but also how to enable the development of innovation within society.[56] Contrary to the common prejudice that the law is an inherent barrier for innovation, the law levels, protects and enforces innovation.[57] Taking both of these effects of law into account, i.e. those restricting the scope of action of risk-causing innovators, as well as those leveling, protecting, and enforcing innovation, Hoffmann-Riem summarizes this approach by posing the essential question: How should legal instruments be shaped in order to enable and even promote innovation without denying necessary protection? From this point of view, only those regulations that do not take particularities of innovation processes into account, and, thus, are badly drafted, are an unjustified barrier for innovation.[58]

2. The regulator's perspective

Referring to theories of evolutionary economics, the research approach that focuses on innovation builds upon modern movements in administrative law that seek to cope with the problem that the regulator has limited knowledge of future events.[59] With respect to German law, Voßkuhle pinpoints the essential differences between this new and the traditional approach by giving a brief summary of its historical development. The tradi-

55 See Hoffmann-Riem, ibid., p. 257.
56 See Hoffmann-Riem, ibid., pp. 256 ff.
57 See, instead of many, Mayer-Schönberger, The Law as Stimulus: The Role of Law in Fostering Innovative Entrepreneurship, pp. 159 to 169; Gasser, Cloud Innovation and the Law: Issues, Approaches, and Interplay, pp. 19 and 20.
58 Hoffmann-Riem, ibid., 260 and 261; cf. also Brownsword and Yeung, Regulating Technologies: Tools, Targets, and Thematics, p. 21.
59 See Hoffmann-Riem, ibid., pp. 259 to 262; Appel, Tasks and Procedures of the Innovation Impact Assessment, p. 149.

tional approach mainly concentrates on the judicial act and examines its conformity with law. This examination is based on a systematic review of positive law and the elaboration of underlying principles. This examination results, in essence, with either a yes or no answer. Its primary aim is binding the executive to the rule of law.[60] Several studies from the 1970's had proved, however, high execution deficiencies of this classic form of imperative public law, particularly in the environmental sector. Upcoming new forms of informal cooperation, between the public and private sector appeared, at the time, to function better than these classic forms of regulation. Researchers started, therefore, to thoroughly investigate the interrelationship between legislative rule making, administrative, as well as judicial decision-making, and its implementation within society. As a main starting point for alternative strategies and forms of regulation, they discovered that the regulator, in particular, did not have the full knowledge of a situation caused by more and more complex environments (particularly in the environmental, telecommunications, and other technique-driven sectors), its increasing non-linear dynamics, and, thus, (objectively) unforeseeable and (sometimes) irreversible effects.[61]

Methodologically, the new regulatory approach ties into the concept of control theory developed in political sciences.[62] Elaborating on this approach, German legal scholars in administrative law usually build on a concept of control focusing on the actions of those individuals or entities that are affected by it. This concept differentiates between the individuals and entities, aim, and instruments of control, as well as the controlling entity. Indeed, the term "controlling entity" should not conceal the fact that there often is no single entity but rather an interactive process that consists of several entities, working together and against each other, and producing regulatory outputs.[63] Similarly, with respect to the individuals and entities affected by the regulation, legal scholars recognize that society finds its solutions for problems in complex structures and a central regulator, in particular the legislator, may have difficulties to appropriately address the individuals in order to achieve its regulatory aims. Keeping this in mind,

60 See Voßkuhle, New Regulatory Approach of Administrative Law, cip. 2 to 8.
61 See the summary of the evolvement at Voßkuhle, ibid., cip. 10 and 11; cf. also Hoffmann-Riem, ibid., pp. 261 to 265; Eifert, New Regulatory Approach of Administrative Law, cip. 1 and 2.
62 See Voßkuhle, ibid., cip. 18.
63 See Voßkuhle, ibid., cip. 20.

the modern regulatory approach nevertheless focuses on the state's point of view and on legislative measures as its main regulation instrument. With these measures, the state seeks to create a certain impact on the individual or entity by focusing on their legal liability should they not adhere to the system. This is the main conceptual difference to the so-called governance perspective, which applies a different point of view that is not restricted in pursuing specific aims by legal means.[64] Focusing on Internet governance, Hofmann, Katzenbach and Gollatz, advocate that the governance perspective instead focuses on reflexive coordination and, thus, "refers to addressing, questioning, and renegotiating Internet-related coordination practices."[65] However, despite or rather because of the analytical difference between both perspectives, the new regulatory approach may refer well to theoretical concepts and empirical findings of the governance approach in order to find out whether "self-regulation" processes already fulfill the regulator's aims or whether there is a need for state regulatory support.

On an international level, legal scholars equally elaborate on the functions, modes, and strategies coming into question for regulation in complex and non-linear environments, however, not always using the same terminology.[66] The common starting point consists in, as mentioned previously, the knowledge deficiencies of regulators acting in these environments. Raab and De Hert describe this common starting point promoting that any understanding of the functioning of regulation (and its "tools") requires one to consider the regulatory activity as a process "in which, in

64 See Eifert, ibid., cip. 5 and 6; Voßkuhle, ibid., cip. 21; cf. also Braithwaite et al., Can regulation and governance make a difference?, p. 3; Hofmann, Katzenbach and Gollatz, Between coordination and regulation: Finding the governance in Internet governance, pp. 6 and 7.

65 See Hofmann, Katzenbach and Gollatz, ibid., p. 13.

66 Cf. Baldwin and Cave, Understanding Regulation – Theory, Strategy and Practice; Raab and De Hert, Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood; Murray, Conceptualising the Post-Regulatory (Cyber)state, with further references, amongst others, to Black, Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a 'Post-Regulatory' World' as well as Scott, Regulation in the Age of Governance: The Rise of the Post Regulatory State', further developed, ibid, The Regulation of Cyberspace – Control in the Online Environment; Franzius, Modes and Impact Factors for the Control through Law; Eifert, Regulation Strategies.

theory, several actors may participate in the making, using, and governing of each tool".[67]

The terminology regarding the regulatory functions, modes, and strategies, is often not comprehensively clear. The German scholar Eifert explains the terminological ambiguity with respect to the diversity of theoretical concepts applied, respectively. He favors to determine, at least, the regulatory strategies pursuant to the state role within the regulation distinguishing, though, between imperative law ("command and control", often also described as "rules), state regulated self-regulation ("co-regulation", often referring to "principles" or "standards"), and societal self-regulation. Focusing on two main types of regulation, i.e. imperative law (command-and-control) and instruments of regulated self-regulation (co-regulation),[68] Eifert sums up the positive and negative aspects of these two types of regulation.

On the one hand a command-and-control regulation provides for high legal certainty (given by the clarity of legal *"if-then*"-rules and the direct effects of its execution). On the other hand, this kind of regulation might be inefficient because it does not take into consideration individuals' economic behaviour. The inflexibility of this kind of regulation constrains more intensively an individual's actions. This restriction leads to three effects: First, it lowers the acceptance of the regulation amongst individuals; second, this increases the probability that the individuals will try to circumvent the regulation; and finally, it increases the efforts of the state to hinder the individuals' circumvention of the law itself. Therefore, this kind of regulation is considered to work best when the following two conditions are met: first, the regulator aims to prohibit third parties' rights or interests being harmed; and, second, the regulator has sufficient knowledge about the effectiveness and efficiency of the corresponding protection instruments. In contrast, if the regulator does not possess sufficient knowledge, such as in a dynamic and non-linear environment, and creativ-

67 See Raab and De Hert, ibid., p. 282.

68 See Eifert, ibid., cip. 13 to 15; focusing on privacy-related principles, Maxwell, Principles-based regulation of personal data: the case of 'fair processing', pp. 212 to 214, referring to J Black, 'Forms and Paradoxes of Principles Based Regulation', LSE Law, Society and EconomyWorking Paper 13/2008, SSRN abstract n8 1267722, L Kaplow, 'Rules Versus Standards: An Economic Analysis' (1992) 42 Duke L. J. 557; R Posner, Economic Analysis of Law (8th edn., Aspen/Wolters Kluwer, New York, 2011), p. 747.

ity is needed in order to solve a variety of problems, this kind of command and control regulation does not provide for the appropriate instruments.[69]

Instead, in order to enhance problem-solving creativity, Eifert stresses co-regulation as the more appropriate regulation strategy. Thereby, taking the decentralized knowledge of private entities into account does not only increase the problem-solving capacities in the society. Rather, the fact that the regulator adapts its regulation instruments to the inherent logics of the entities acting on the private market also increases their acceptance of the regulation instruments. Furthermore, this kind of regulation decreases the administrative costs because the private structures used for it are often also financed privately. Finally, instruments of co-regulation can provide a solution for the territorial problem of "command and control" regulation because its execution does not depend, at least not directly, on the State but private entities not being bound to national territories.[70] However, a possible disadvantage is that this kind of regulation does not meet the regulator's expectations but, instead, makes the regulation more complex, opaque and less effective or efficient than the classic form. Another risk is that the regulated private entities abuse their knowledge advantage toward the State. This could be the case, for example, if the State gives privileges to these private entities because it thinks that their solutions really serve society, but in reality serves their particulars interests, only.[71]

In any case, Eifert stresses, like Franzius, that the complexity of this form of regulation requires the regulator to learn. This means to frequently evaluate its effectiveness and efficiency of its regulation instruments.[72] Such an evaluation should refer to other disciplines, such as to social and economic sciences, and build upon their validated knowledge. The moment when the legislator extends its view to the effects of its regulation, reference to these other disciplines and their methodologies included will increase the rationality of law.[73]

69 See Eifert, ibid., cip. 25 and 26.
70 See Eifert, ibid., cip. 59.
71 See Eifert, ibid., cip. 60.
72 Cf. Eifert, ibid., cip. 60; Franzius, ibid., cip. 81 to 103.
73 See Hoffmann-Riem, Innovation Responsibility, p. 39.

3. Possible pitfalls taking the effects of regulation instruments into account

In conclusion, Voßkuhle summarizes the promises and possible pitfalls of this legal research approach seeking to gain deeper knowledge about the complex effects of law as a regulation instrument. He considers the promises as: first, this approach broadens the scope in which the law is just one regulation mechanism amongst others, such as beside further mechanisms of economic markets, networks or within organizations; second the approach enables researchers to ascertain and take the effects and efficiency of legal instruments into account, and their interplay with further mechanisms; and third, in doing so, the approach enables legal researchers to interconnect with other research disciplines. This last aspect enables researchers to build on theoretical frameworks and empirical methodologies already elaborated on in other disciplines. However, the possible pitfalls of this approach are: On the one hand, legal scholars considering the effects of regulation instruments may over-simplify the complex interplay of cause and effect. The reason is that all theoretical models mirror just one part of the reality and the choice of regulation instruments based on them thus runs the risk of not being able to meet the legislator's goal. On the other hand, the regulatory function of the law is not the only function. The law also serves as an expression of the values provided for by the constitution. This means that legal provisions do not lose their validity just because in some circumstances it has little effect, only, for example, because of inefficient execution of the law.[74]

These considerations are important for the examination of the principle of purpose limitation pursued in this thesis. The principle of purpose limitation suffers, indeed, from a lack of execution in the private market. And this may result from the uncertainty about its precise meaning and extent.[75] However, this lack of execution does not mean, per se, that the principle of purpose limitation should be abandoned as a whole. This hesitation is particularly justified because the uncertainty about its meaning and

74 See Voßkuhle, ibid., cip. 22 to 28.

75 See, in general, the above-mentioned studies as well as, in particular, the observations made in the HIIG Law Clinic where startups simply went on developing their products if they could not definitely clarify how to apply the principle of purpose limitation and expected that data protection authorities would not become aware of their practice, anyway.

extent is not a special problem of the principle of purpose limitation but of all legal principles in general. The less imperative law and its conditional if-then-scheme serves as regulation instrument, the more important instruments, such as legal principles, become. Principles do not provide for a binary scheme that will answer the question of whether an act is legal or not but allows individuals to explore different, and in the best possible outcome an optimal solution.[76] Indeed, with the abandonment of imperative law and its conditional decision rule, the individuals' legal uncertainty increases because individuals do not know whether the solution found meets the regulators expectations. Consequently, individuals and the regulator have to start an interactive process reconstructing together, the certainty of legal rules.[77] The answer of whether or not or in which way the regulator meets its expectations regarding the principle of purpose limitation depends, in the first instance, on the above-mentioned research questions of this thesis.

III. Course of examination

In order to answer the research questions, the next chapter clarifies the conceptual definitions which provides a basis for regulation of innovation. The first sub-chapter illustrates how economic theories define and conceptualize "innovation" and "entrepreneurship" and which role the law plays in these conceptualizations of "innovative entrepreneurship". In doing so, one particular focus is on the illustration of economic models describing the non-linearity of innovative entrepreneurship processes. Subsequently, the examination goes on to review literature from both economic and legal perspectives and examines the effects of legal certainty on "innovative entrepreneurship". The first sub-chapter concludes with the appearing regulatory conflict: On the one hand, as discussed, regulation instruments, such as the principle of purpose limitation, is open toward innovation but decreases legal certainty; on the other hand, legal uncertainty hinders innovation. Therefore, it will be key to explore mechanisms that combine both aspects, i.e. being open toward innovation but also ensuring legal certainty and, thus, even promoting innovation. The second sub-chapter draws at-

76 See Franzius, ibid., cip. 7; cf. Raab and De Hert, ibid., p. 278.
77 Cf. Franzius, ibid., cip. 17.

tention to the other side of the "innovation" coin, i.e. data protection law as a regulation of risks caused by innovation. This sub-chapter clarifies the terms "risks" and "dangers", as well as the often correspondingly used protection mechanisms "prevention" and "precaution". This distinction is highly relevant for exploring the function of the principle of purpose limitation at a later stage. The discussion on various protection instruments for different types of threats leads to the last sub-chapter that clarifies the conceptual definitions for the regulation of data-driven innovation: The question of what is threatened, in terms of data protection and, thus, which object of protection the principle of purpose limitation serves. Based on Nissenbaum's work *Privacy in Context*, this last sub-chapter provides an overview about the prevailing theories, concepts, and approaches on the value of privacy. So far, this work does hence not yet clarify the distinction between privacy and data protection and, correspondingly, privacy and data protection laws; this distinction is an essential element of the conceptual work of this thesis and will be proposed later on. This sub-chapter finally gives a first response to Nissenbaum's critique on the purpose-oriented concept of protection by clarifying the relationship between the terms "purpose" and "context". This will lead to a first insight into the function of the principle of purpose limitation.

The third chapter contains the main part of this thesis: An analysis of the legal framework determining the meaning and function of the principle of purpose limitation. Elaborating on the object and concept of protection of data protection law, this chapter seeks to clarify three main question: first, the precise meaning and extent of the requirement to specify the purpose; second, the precise meaning and extent of the requirement to limit the later use of data to the purposes originally specified; and third, which specific instruments are appropriate for establishing these two requirements in the private sector in order to find a sound balance between enabling innovation and protection against its risks in society. In doing so, the first sub-chapter clarifies the interrelationship between the different regimes of fundamental rights focusing on the European Convention on Human Rights (ECHR), the European Charta of Fundamental Rights (ECFR), and German Basic Rights (GG). Furthermore, it treats the question of the effects of these fundamental rights in the private sector, in particular, of the right to privacy under Article 8 ECHR, the rights to privacy and data protection under Article 7 and 8 ECFR, as well as the German right to informational self-determination under Article 1 sect. 1 in combination with 2 sect. 1 GG. The question is whether these fundamental

rights directly bind private entities that process personal data, like the State, or whether they have only an indirect effect in the private sector. The thought behind this question is that the second alternative gives the legislator more room for transposing the constitutional requirements into secondary and/or ordinary law. The sub-chapter goes on to analyze the object and concept of protection developed by the European Court of Human Rights (ECtHR), the European Court of Justice (ECJ), and the German Constitutional Court (BVerfG), with respect to each of the above-mentioned fundamental rights. This parallel analysis will effectively allow one to compare the differences between the corresponding objects, as well as concepts of protection. The first sub-chapter concludes with an analytical result on the challenges facing, in general, from these objects and concepts of protection being very broad and vague. A theoretical solution provides a first hint on how this may also affect the determination of the function of the principle of purpose limitation.

The next sub-chapter draws the attention to the main problem resulting from such concepts of protection that are intrinsically broad and/or vague: The uncertainty about how to legally specify the purpose of the data processing. On a European level, the analysis will illustrate that there are almost no criteria which help specify the purpose, provided for by the judicial courts in light of the corresponding fundamental rights. However, it will be illustrated that the specification of the purpose is an essential element in secondary law because several further definitions and requirements, such as the scope of application, refer to the purpose specified. Despite this essential role, the Article 29 Data Protection Working Party, having an advisory status for questions about the interpretation of the Data Protection Directive, does not provide reliable criteria for the specification of the purpose, either (nor does the General Data Protection Regulation address this issue). Therefore, the sub-chapter continues to examine how the secondary law itself specifies certain purposes of processing such as for "marketing electronic communications services", pursuant to Art. 6 sect. 3 of the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). Subsequently, the examination turns into the question of how the German legislator transposes these requirements into German ordinary law. This allows the comparison, since there are almost no criteria provided for by European fundamental rights, of the concept of protection established within ordinary law, at least, with German basic rights. The

analysis of European secondary and German ordinary law, as well as its comparison with the (so far developed) constitutional requirements, alludes to the fact that there are several flaws in the concept of protection. The results not only confirm the general challenges stemming, as concluded previously, from the object and concept of protection as being very broad and vague, now with particular respect to the requirement of purpose specification. Rather, it is apparent from the results that these flaws consist, in essence, in the fact that the constitutional requirements for the processing of data by the State are, in essence, equally applied to private entities. Since private entities have different means for specifying purposes at their disposal than the State, this leads to the situation that the effects of the requirements are even stricter for private entities than for the State. This sub-chapter hence concludes, with a particular focus on the European Charta of Fundamental Rights, with a refinement of the object and concept of protection serving a better scale to private entities for the specification of the purpose of their data processing.

The following sub-chapter treats the second component of the principle of purpose limitation, i.e. the question on the precise meaning and extent of the requirement to limit the later processing to the purpose(s) initially specified. The examination exemplifies two different models: The European model of purpose compatibility and the German model requiring strict purpose identity allowing, however, a change of purpose if this change is proportionate. With regard to the European model, this doctoral thesis examines the criteria developed by the European Court of Human Rights, as well as the European Court of Justice in light of the corresponding fundamental rights. While the European Court of Human Rights mainly refers to the "reasonable expectations" of the individual concerned by the processing of data related to him or her, the European Court of Justice does not. Interestingly, the Article 29 Data Protection Working Party nevertheless refers, proposing their criteria helping answer the extent of the requirement of purpose compatibility, to the individual's "reasonable expectations",[78] albeit the Data Protection Directive does not either (interestingly, Article 6 sect. 4 lit a-e of the General Data Protection Regulation also lists all criteria but the "reasonable expectations" criterion). It is apparent from the analysis that the criteria proposed do not actually help in

78 See the Art. 29 Data Protection Working Party, Opinion 03/2013 on the principle of purpose limitation, pp. 24 and 25.

answering the question on the extent of the requirement of purpose compatibility. This doctoral thesis therefore continues, in order to receive inspiration on which functions the limitation of purposes can have, to examine the German model. Interestingly, albeit German ordinary law transposes the European directive, it deviates, at least formally, from the compatibility requirement. The examination therefore draws the attention to the concept of protection provided for by the German basic right to informational self-determination in order to find the reason for the deviation. Since the reason for the deviation appears to come, indeed, from the application of the German basic right (and not of the European fundamental rights), this thesis presents three alternative approaches proposed within German legal literature in order to get a clearer understanding about the possible functions of the principle of purpose limitation. Indeed, all three approaches refer to the processing of data by the State. Taking the results of the preceding analysis into account, the thesis concludes this sub-chapter with a new approach defining the meaning and extent of the principle of purpose limitation for the private sector.

On the basis of the own approaches developed in the two last-preceding sub-chapters, the last sub-chapter treats the question of which specific regulation instruments serve best in order to establish this new understanding of the meaning and extent of the principle of purpose limitation in the private sector. Here, the thesis exemplifies, iteratively, the impact of this understanding on the following elements: first, the scope(s) of application of all protection instruments; second, the specific application of the protection instruments in the private sector (in particular, the necessity as well as interplay of the individual's consent and other legitimate basis laid down by law); and third, on particular aspects of the consent, its withdrawal, and a right to object to the data processing, as well as on further protection instruments such as rights of information, participation, and deletion of personal data, by taking the individual's decision-making process as a whole into account.[79]

Finally, on the basis of the refined concept of protection regarding the principle of purpose limitation and related protection instruments, the last chapter of this thesis comes back to answer questions about the effects of these instruments. These questions refer to both sides of the "innovation"

79 Cf. the concept and terminology of "choice architectures" at Thaler and Sunstein, Nudge – Improving Decisions About Health, Wealth, and Happiness.

coin, i.e. the effects on processes of "innovative entrepreneurship" as well as on the efficiency of risk protection instruments. The preceding chapters will have made certain remaining questions apparent that cannot sufficiently be answered by legal analysis alone. This last chapter therefore proposes an empirical methodology that helps answer the remaining questions. On the basis of these results, the regulator might answer the overarching question of which instruments fits best its regulatory aims.