Data Screening as a Means of Preventing Islamist Terrorist Attacks on Germany

By Wilhelm Achelpöhler and Dr. Holger Niehaus[*]

After the terrorist attacks on the World Trade Center in New York City, it was determined that some of the presumed perpetrators had lived in Germany where they had been studying technical subjects in particular. Public authorities supposed more potential assassins (so-called "sleepers") were staying in Germany until they received an order to start their mission. In order to discover such persons, data screening[1] was carried out in each federal state of Germany. In the course of it, all universities were obliged to hand over the data material concerning their enrolled students for data alignment by police authorities. Up until now, appeals of affected students against those measures have been successful in Hessen, Nordrhein-Westfalen and Berlin. Those events give reason for a critical reflection of the means of data screening by the police.

A. The Concept of Data Screening

As data screening the ascertaining of information by aligning is described; these information result from two different amounts of data at least.[2] By such an alignment, an intersection of information is found ("substrate" or, "sediment") which either already meets the aim of the investigations or allows it to continue with conventional methods.[3] The strategy of investigation is either aimed at achieving wanted information ("positive data screening") or selecting insignificant informa-

[*] Wilhelm Achelpöhler is a partner of a law firm in Münster (Achelpoehler@meisterernst.de). Holger Niehaus works as an assistant lecturer at the University of Münster (Institute for Criminal Law; niehauh@uni-muenster.de).

[1] "Rasterfahndung"; a "rastrum" (lat.) is a rake, by which disordered things can be sorted or separated. Welp, *Zur Legalisierung der Rasterfahndung, in* RECHT DER PERSÖNLICHKEIT 389 (Berlin 1996).

[2] NIEHAUS, KATALOGTATENSYSTEME ALS BESCHRÄNKUNGEN STRAFPROZESSUALER EINGRIFFSBEFUGNISSE 145 (Berlin 2001).

[3] Welp, *supra* note l, at 389; Wittig, JuS 1997, 961, 968; Niehaus, *supra* note 2, at 145-6.

tion ("negative data screening").[4] Because of the use of electronic data processing this kind of clearing up crime has achieved unknown effectiveness.

At the same time, the available quantity of information is increasing unstoppably as we morph into an information society.[5] Regarding the development of cashless exchanges of money, for instance, one can state that today every single user of EC cards or credit cards leaves a trail of data behind for investigating officers. For example, it could be discovered which persons bought the same type of knife recently used by a murderer.

Even originally irrelevant data gains unexpected significance due to the possibilities of automatic data processing and its capacity of handling and connecting items.[6] If one knows, for example, that a member of a terrorist organisation acting in Germany sent a blackmailing letter from Gare du Nord in Paris, and if one additionally knows that the members of that terrorist organisation prefer paying their electricity bills in cash, the separately considered insignificant data about who travelled to Paris by train lately and who paid his electricity bill in cash achieve, a so far, unimagined importance. Aligning those two pieces of data, an intersection of persons can be found to which both the search criteria apply. Concerning the remaining number of persons investigations can be continued with usual Observation methods. Conclusively, data screening serves to select a manageable number of persons with characteristic features from an inestimable variety of information by data alignment.[7]

B. Data Screening and Basic Rights

I. The right to data privacy

The development of information technologies poses new kinds of threats to personal rights. A citizen, when he considers which public authority knows with whom, what, when and where he acts is already hampered by that uncertainty concerning his freedom of action.[8] People who are unsure whether divergent be-

---

[4] Welp, *supra* note 1, at 389.

[5] Welp, *supra* note, at 389-90; SOKOL, POLIZEI UND DATENSCHUTZ, 188, 196 (in Bäumler, ed. Neuwied 1999); Niehaus, *supra* note 2, at 146.

[6] BVerfG 65, 1 (45).

[7] Welp, *supra* note 1, at 389-90.

[8] BVerfG 65, 1 (43); BVerfG 27, 1 (6).

haviour is noted and is durably stored, used and passed on, will try not to attract attention by such behaviour.[9]

Therefore, the Federal Constitutional Court deduces the right to self-determination about personal data from the general personal rights (Art. 2 (1) in conjunction with Art. 1 (1) GG). The right to self-determination about personal data means that one can decide, on principle, anything concerning the divulgence, the use, and the passing on of one's personal data.[10]
Regarding the level of intrusion, the Federal Constitutional Court does not differ any more between the especially delicate data of the personal sphere of life (e. g. medical data about existent illnesses) and the less delicate data of its social sphere (e. g. matriculation at a university). Due to the possibilities of modern data processing, even separately considered insignificant data can gain real importance in other connections because of the new ways of connecting and processing information. In this respect there is no "insignificant" data left in times of automatic data processing.[11] Therefore, any poll, storage or passing on of personal data, even the fact that the state simply takes note of them, means an intrusion into the right to data privacy.[12]

II. The intrusion degree of data screening

The importance of an intrusion into the basic rights of a citizen by the police or in criminal proceedings, on the one hand, can result from the intensity of the infringement of freedom, on the other hand, from its secret enforcement, but as well from the circumstance that numerous uninvolved persons are referred to ("spread" of intrusion).[13] Related to these criteria, data screening means a serious intrusion into the right to data privacy.[14] Data screening not necessarily refers to especially sensitive data. Therefore, its importance does not inevitably result from the intensity of the infringement of freedom. However, as the persons affected neither are informed nor have been heard, data screening is regularly carried out secretly (but not necessarily secretly, as data screening concerning Islamist terrorists showed in 2001). Inherently, it has to be classed among intense intrusions. Mainly, the secret

[9] BVerfG 65, 1 (43).

[10] *Id.*

[11] BVerfG 65, 1 (45).

[12] Di Fabio, MAUNZ / DÜRIG, GRUNDGESETZ, (39th supplement, 2001), Art. 2, annotation 176.

[13] Welp, *supra* note 1, at 392.

[14] Welp, *supra* note 1, at 389, 414; Niehaus, *supra* note 2, at 200; Sokol, *supra* note 5, at 192.

collecting and processing of data can easily evoke uncertainty among the citizens about what different public authorities know about them. Particularly, that creation of uncertainty has induced the Federal Constitutional Court to develop the principles of data privacy. [15]

Decisively, its extraordinarily high spread shows that data screening must belong to the intense intrusions into the basic rights of a citizen.[16] To be successful, data screening inevitably requires access to the data of an unmanageable great number of uninvolved persons (of the entire population, in the extreme case), who are not at least suspected. In the course of the data screening following the terrorist attacks in New York City, merely in *Nordrhein-Westfalen* (Northrhine-Westphalia), data of 5 million males was collected.[17] Therefore, viewed from the standpoint of spread, data screening is a mass-intrusion into the fundamental rights of all citizens, which cannot be compared with any other intrusion into fundamental rights carried out by the police or in criminal proceedings.[18]

C. Statutory Sources

Related to criminal proceedings, data screening is regulated in § 98 a of the criminal procedure code ("Strafprozessordnung", "StPO") since 1992. Related to the police, its legal basis partly was established in 2001 in order to authorize the data screening at the universities (e.g. in Schleswig-Holstein, Bremen and Niedersachsen). The legal bases for the police[19] do not inconsiderably differ regarding their premises.

I. The order competence

In several federal states of Germany the realization of data screening is dependent on the order by the district court judge ("judicial retention").[20] However, in other

---

[15] BVerfG, 65, 1 (43).

[16] Welp, *supra* note 1, at 389, 414; LG Wiesbaden, 4 T 707/01, 3 (6 Feb. 2002); Niehaus, *supra* note 2, at 200.

[17] WESTFÄLISCHE NACHRICHTEN, (No. 31) 6 Feb. 2002, at RMS 1.

[18] Welp, *supra* note 1, at 389, 414; Strate, ZRP 143-4 (1990); Wolter, GA 129 (1988); Möhrenschlager, WISTRA 1992, 326.

[19] Art. 44 bay. PAG; § 40 bad-württ. PolG; § 47 ASOG (Berlin); § 46 PolG (Brandenburg); § 36 i BremPolG; § 23 Hamb. GesDatVPol; § 26 SOG Hessen; § 44 SOG M-V; § 45 a NGefAG (LT-Dr. 14/2730); § 31 PolG NRW; § 25 d POG (Rheinland-Pfalz); § 37 Saarl. PolG; § 47 Sächsisches PolG; § 31 SOG (Sachsen-Anhalt); § 195 a LVwG (Schleswig-Holstein, draft: LT-Dr. 15/1267, p. 4); § 44 PAG (Thüringen).

[20] § 47 ASOG Berlin; § 46 PolG (Brandenburg); § 26 SOG Hessen; § 31 PolG NRW; § 31 SOG (Sachsen-Anhalt); § 195 a LVwG (Schleswig-Holstein, draft: LT-Dr. 15/1267, p. 4).

federal states of Germany, the head of the State Bureau of Criminal Investigation is responsible;[21] sometimes even the agreement of the Secretary/Senator of the Interior is required.[22] In Mecklenburg-Vorpommern only the Ministry of the Interior is competent.[23]

II. Pre-condition of a future peril

Concerning the degree of danger which is required to carry out data screening, and regarding the reference objects of danger, there are different statutory sources, as well.

1. Almost all statutes demand an actual danger. Only in Bavaria, Baden-Württemberg and Niedersachsen the simple danger of a future criminal act of considerable importance is sufficient.[24] In Schleswig-Holstein a considerable danger is required.[25]

2. In most German Federal States, the reference objects of danger only are the survival or the safety of the Federal Government or a federal state as well as a person's life, physical integrity or freedom.[26]

In addition, partial data screening is declared legal to prevent a criminal act of considerable significance.[27] In Rheinland-Pfalz a considerable danger is necessary, although reference to a specific object of danger is not required does not have to be referred to.[28]

---

[21] § 40 bad-württ. PolG; Art. 44 bay. PAG; § 36 i BremPolG; § 23 Hamb. GesDatVPol („Präses bzw. Staatsrat der für die Polizei zuständigen Fachbehörde"); § 45 a NGefAG; § 25 d POG (Rheinland-Pfalz); § 37 Saarl. PolG; § 47 Sächsisches PolG; § 44 PAG (Thüringen).

[22] § 40 bad-württ. PolG; Art. 44 bay. PAG; § 36 i BremPolG; § 45 a NGefAG; § 47 Sächsisches PolG; § 44 PAG (Thüringen).

[23] § 44 SOG M-V.

[24] § 40 bad.-württ. PolG; Art. 44 bay. PAG; § 45 a NGefAG.

[25] § 195 a LVwG Schleswig-Holstein.

[26] § 47 ASOG Berlin; § 46 PolG Brandenburg; § 23 GesDatVPol Hamburg; § 26 SOG Hessen; § 44 SOG M-V; § 31 PolG NRW; § 37 PolG Saarland; § 31 SOG Sachsen-Anhalt; § 195 a LVwG Schleswig-Holstein; § 44 PAG Thüringen.

[27] § 40 bad-württ. PolG; Art. 44 bay. PAG; § 36 i BremPolG; § 45 a NGefAG; § 47 sächs. PolG.

[28] § 25 d POG Rheinland-Pfalz.

III. Judicial Remedies

There is a direct connection between two relevant elements: the question concerning the competence of ruling and the question referring to judicial remedies for an indictment against the ruling of data screening. On principle, according to §40(1) of the administration procedural code ("VwGO") the administrative courts are responsible for indictments against preventive measures taken by the police.

1. The Competency of the Court

However, if a district judge ("Amtsrichter") is responsible for the ruling of data screening the legal process is arranged according to "FGG"-code of procedure.[29] Consequently, an appeal to a district court ("Landgericht", "LG") and a further appeal to the appellate court ("Oberlandesgericht", "OLG") is permitted. On the other hand, if the chief officer and/or the Secretary/Senator of the Interior got ruling competence,[30] then the Administrative Court remains responsible.

2. The Range of Judicial Remedies

The range of a judicial decision in the appeal procedure depends if there is judicial retention. If the decision of the county court that ordered data screening is reversed by an appellant process, then, at the same time, the police's application for ruling data screening is rejected. In consequence, data screening must be stopped completely, as one of its requirements is missing; the ruling of the court.[31] If there is only the retention of a chief officer and if an administrative court declares data screening illegal in connection with a lawsuit of a person affected, this judgement is effective only between the parties ("inter partes"). The ruling of data screening remains in force for the other persons affected. Theoretically, authorities could continue data screening all persons affected, except for the successful plaintiff. In any case, data screening would not have to be stopped after a decision by the first court.

D. Do the Statutory Regulations Comply with the Constitutional Requirements?

According to the adjudication of the Federal Constitutional Court, the state legislator must establish statutory pre-conditions for data screening by the police in order

[29] *E.g.* § 31 (4), 3 PolG NRW.

[30] § 40 bad-württ. PolG; Art. 44 bay. PAG; § 36 i BremPolG; § 23 Hamb. GesDatVPol; § 45 a NGefAG; § 25 d PolG Rheinland-Pfalz; § 37 Saarl. PolG; § 47 Sächsisches PolG; § 44 PAG (Thüringen).

[31] LG Wiesbaden, 4 T 707 / 01 (6 Feb. 2002).

to guarantee the prine of proportionality.[32] A statute which failed to do so, and would leave the judgement whether the procedure satisfies the demands of the principle of proportionality to the administering authorities, would offend the right to data privacy and therefore would be unconstitutional.[33]

I. The Requirement of a "Danger"

Unlike the data screening based on the criminal procedure code (§ 98 a StPO) that requires a suspicion of a past offence, the data screening based on police law only requires a danger to certain subjects in the future. To prevent this danger, the police are allowed to collect and screen data of an indeterminate multitude of persons who need not bear a specific closeness to the dreaded danger. Therefore, data screening based on police law would be allowed, without any limitations, if the statutes do not demand restrictive pre-conditions.[34] A statute that would allow data screening in any case of danger for public safety would not meet the requirements of the constitutional principle of proportionality. As mentioned before, the state laws require increased levels of danger according to the principle of proportionality.

1. Danger of a future substantial offence / substantial danger

If some state laws only demand a certain reference object for the danger by demanding a danger of a "future substantial offense" or a "substantial danger", this law cannot be deemed a real restriction. Facing the extensive costs and manpower that data screening requires, the police will not use this method for preventing minor offenses (e.g. shoplifting). But even the theft of a locked bicycle (§243 of the criminal code ("StGB")) is - in cases of professional perpetration - already a "substantial offense" (e.g. §8(3) No. 1 of the police law code of Nordrhein-Westfalen ("PolG NRW"); § 2 No. 10 c) of the police law code of Niedersachsen ("NGefAG"). Therefore, the condition "substantial offence" does not achieve anything beyond the general principle of proportionality, which the method has to meet anyway.[35]

---

[32] BVerfG 20, 162 (187); Rudolphi, *introduction to § 94, in* SYSTEMATISCHER KOMMENTAR ZUR STRAFPROZESSORDNUNG, annotation 68; Welp, *supra* note 1, at 389, 411; Degener, Grundsatz der Verhältnismäßigkeit und strafprozessuale Zwangsmaßnahmen, Berlin 1985, p. 203; Niehaus, *supra* note 2, at 188.

[33] LVerfG Mecklenburg-Vorpommern, 2 (98).

[34] Sokol, *supra* note 5, at 188, 192.

[35] Welp, *supra* note 1, at 407; Niehaus, *supra* note 2, at 169.

2. Present Danger to an Important Subject of Protection

In fact, the intrusion into privacy of a multitude of persons by data screening can only be proportional if a higher grade of probability exists that a danger will realise. Therefore, most of the state police law codes rightly require a present danger (i.e. circumstances, where the danger has already begun to realize or is imminent with a high level of probability). Furthermore, the plentiful access to data of countless unsuspected people must not occur to prevent *any* danger. In fact, data screening is only proportional if it is used to protect outstandingly high-ranking subjects. Therefore, the principle of proportionality requires an increased level of danger and outstanding high rank of the subject of protection.

Thus, only the state police laws which allow data screening only to prevent a present danger and only if a high-ranking subject of protection is endangered, are proportional and complying with the constitution (e.g. life, liberty or physical integrity of a person or integrity of the federation or a federal state).

II. Order Competence

Due to the character of data screening as a plentiful intrusion into the rights of completely uninvolved people, the larger part of the affected persons will not be made aware of the screening. With regard to these persons, factually, data screening is a clandestine method. On the other hand, Article 19 IV of the German Basic Law ("Grundgesetz") requires effective legal protection against governmental procedures that cannot be given if the affected persons do not know of the screening of their data.[36] Therefore, clandestine methods based on criminal procedure law regularly require an authorisation by judge (cp. §§ 98 b, 100 b, 100 d StPO). Thereby, a judicial control can be achieved at least in the forefront of the procedure.[37] There are no differences concerning clandestine intrusions into base rights founded on police law.

1. Order by Chief Officer as a Sufficient Control?

Some federal state laws reserve the order competence to the chief officer of the police. Thereby, in many cases, the procedure will be deprived of judicial control. The chief officer is part of the executive branch; therefore, with regard to the necessity of prior legal protection by a neutral judge, his prior participation is irrelevant. Consequently, concerning legal protection, there are doubts about the constitution-

[36] OLG Düsseldorf, 3 Wx 357 / 01, 5 (8 Feb. 2002); VerfGH Sachsen, JZ 1996, 957, (963-4).

[37] *Cf.* VerfGH Sachsen, JZ 1996, 957 (963).

ality of those state laws which merely demand an order by the chief officer for data screening.

2. Advisability of the Assignment of the Order Competence to the Regular Courts

As far as the state laws reserve the order competence to the courts, they assign this task to the regular courts ("*ordentliche Gerichtsbarkeit*"). For procedures based on criminal procedure law, this assignment is a matter of course. However, it is questionable why the state police laws, too, assign the order competence to the regular courts. Concerning imprisonment, this assignment might be sensible[38] because the arrest warrant is often requested with short notice and therefore, can better be issued by the nearby county courts. Furthermore, these courts are competent in other cases of imprisonment, as well (cp. § 3 of the code concerning the judicial procedure referring to imprisonment).

However, these considerations do not apply to a data screening-order. Reasons why it should not be under examination of the administrative courts, which are competent for matters of police law, are not apparent. In fact, several practical problems arise from the assignment of competence to the regular courts. For example, in 2002, a district court decided on an appeal against data screening asked the appellant for duplicates of the quoted police law-literature because it was not available in the library of the district court. Furthermore, the "FGG"-code of procedure does not follow with the specifics of police law based intrusions into basic rights. For example, according to the wording[39] of the statute, there is no claim for the subsequent ascertainment of illegality, if the procedure is finished in the meantime – which often is the case concerning police procedures. In the administration procedural law code ("VwGO") § 113(1)4 would be at disposal.

3. Efficiency of the Requirement of a Judicial Order as a Protection-Mechanism for Basic Rights

Considering the efficiency of the requirement of a judicial order as a protection-mechanism for basic rights, the assignment of competency to the regular courts must be criticised as well. In the range of intrusion into basic rights based on criminal procedure law (e.g. telephone surveillance), according to researches of the Federal Ministry of Justice, not a single case existed where county courts dismissed an

[38] *E.g.* § 36 PolG NRW.

[39] Therefore, subsequent legal protection has to be created through constitutional considerations by the courts (*cf.* OLG Düsseldorf, 3 Wx 357/01, 5 (8 Feb. 2002)).

application.[40] One reason for this might be that these proceedings (so called "GS"-proceedings) are not credited for the workload of the judge. Furthermore, the county court judge has to face matters (police law) which do not belong to his usual competency. Under these circumstances the county court judge will often simply trust the information given by the police and grant the application. Considering these facts, the requirement of a judicial order by the county courts cannot be deemed a serious control of the methods.[41]

The inefficiency of the present pre-condition of a judicial order as a protection-mechanism can be shown by the development of judiciary in the present legal discussion about the legitimacy of data screening. While not a single county court judge dismissed an application by the police, the higher courts later partly criticised that the applications were solely based on suppositions and did not get beyond speculations.[42] Such deficiencies must have had been recognised by the county courts if they had seriously examined the applications.
Therefore, the efficiency of judicial control begs for an assignment of the prior judicial order to the administrative courts.

E. Data Screening after the Attacks in New York City

Investigations after the terrorist attacks in New York resulted in a delinquent profile, which included the following characteristics: male, 18 years old at least, 41 years at the most, Islamic, student or former student, valid permit of residence without any local restriction, unknown to the police, no children of his own, financially independent (not understandable, irregular deposits in the bank account).[43] After data screening had been ordered in all federal states, among others the universities were forced to hand over the data of their enrolled students. The scope of that data diverged from one federal state to the other. For instance, in Berlin only the data of citizens from 15 countries had to be given to the authorities,[44] in Nordrhein-Westfalen, however, the data of all male students between 18 and 41 was required.

---

[40] Thommes, StV 1997, 657, 660 and 664; Welp, Festschrift Mangakis, Athens 1999, pp. 809, 814; BT-Dr. 12 / 8396, p. 3; BT-Dr. 13 / 6689, p. 5; BT-Dr. 13 / 7341, p. 5.

[41] Dencker, *Organisierte Kriminalität und Verfassungsstaat*, *in*: RECHTSSTAAT IN DER BEWÄHRUNG, Vol. 33, 41, 55 (Albrecht & Dencker et. al., Heidelberg 1998); Welp, StV 1994, 161, 163. In the same way Götz, JZ 1996, 969, 970; Lisken / Mokros, NVwZ 1991, 609.

[42] LG Wiesbaden, 4 T 707 / 01, 4 (6 Feb. 2002).

[43] AG Wiesbaden, 71 GS 531/01 (25 Nov. 2001).

[44] FRANKFURTER RUNDSCHAU, (No. 242) 18 Oct. 2001, at 6.

I. Order Premises

As in numerous federal states, students affected filed suit due to the data screening, the courts had to find out whether there was a valid premise allowing data screening. In most federal states an actual peril for the survival or safety of the Federal Government or a single federal state or for a person's physical condition, life or freedom is required for data screening.

1. Actual Peril

A definition of the term "actual danger" can be found in §2 NGefAG: According to it "actual danger" means a danger where the effect of the harming event has already started or where it is about to start or will start the next time. Therefore, a latent or potential peril, where actual dangerousness does not presently exist, but where a later emerging source of danger cannot be precluded,[45] is not satisfactory. Comparing all grades of danger "actual danger to life or physical condition" is the ultimate threat.[46] So, facts are necessary to justify the prognosis that subjects of protection are endangered by life, physical condition or the safety of the Federal Government and of the federal states. The required actuality of danger demands that the endangering of the subjects of are endangered by mentioned above has either already started or will with the utmost probability, at least, will start immediately or in the very next time.[47]

2. Danger for domestic subject of protection

It has to be stressed that the subjects of protection must be in actual danger in the respective federal states, as only then may police of the respective state act. So, the assumption that persons who stay in Germany might plan further attacks in the USA is not a suitable ground for actual danger. A repressive data screening for use in criminal proceedings based on § 98a StPO could have been undertaken when there was an initial suspicion for one of the offences enlisted in § 98a StPO (e. g. the foundation of a terrorist association, § 129a StGB). The federal states of Germany have not made use of that possibility, instead, they decided for the means of preventive statutory sources (i.e. police law).

---

[45] *Cf.* LISKEN & DENNINGER, HANDBUCH DES POLIZEIRECHTS, chapter E, annonation 51.

[46] Lisken & Denninger, *supra* note 45, at chapter E, annotation 47; LG Wiesbaden, 4 T 707/01, 3 (6 Feb 2002).

[47] Lisken & Denninger, *supra* note 45, at chapter E, annotation 43.

II. Legal discussion

The courts which have dealt with the issue of actual danger reached different conclusions.

1. The district court ("*Amtsgericht*", "AG") of Düsseldorf[48] takes the following view: The required certainty of damage decreases as the extent of the possible damage increases.. The terrorists responsible for the attacks in New York would accept the death of thousands of people. As some of the supposed supporters of Osama Bin Laden had been living in Nordrhein-Westfalen, danger would exist there, too, even if an immediate attack could not surely be predicted at the moment.

2. The regional court ("Landgericht", "LG")[49] and the appellate court ("Oberlandesgericht", "OLG") of Düsseldorf[50] have accepted the explanation of the *Amtsgericht*. As the Federal Government declared its unrestricted solidarity with the United States´ course of action and as Islamist terror organisations announced to exercise measures of retaliation against the states taking part in military actions, an actual danger to the safety of the Federal Government or a federal state must exist. However, the OLG Düsseldorf considers the ruling of data screening concerning German citizens to be disproportional (cf. 3, below).[51]

3. The *Verwaltungsgericht* (administrative court) Mainz, also held the requirement of the existence of an actual peril to be fulfilled.[52] In contrast to the courts in Nordrhein-Westfalen, it did not find a state of danger to German subjects of protection existed, but it permitted data screening in order to fight dangers outside of Germany as well. This is based on Art. 1 (2) GG, which included an pledge of the state to support the worldwide realization of human rights.[53] Contrary to the legal position of most other federal states, in *Rheinland-Pfalz* (Rhineland-Palatine) a restriction on the specific objects of actual danger is missing. Consequently, data screening can be used for preventive measures to combat crime. According to § 6 StGB ("Weltrechtsgrundsatz"), German criminal law is applicable for crimes caused by explosives (§§ 308 (1) – (4), 309 (2), 310 StGB), so the *Verwaltungsgericht* Mainz believes it to be sufficient that the expected criminal act may occur in a foreign country.

---

[48] AG Düsseldorf, 151 Gs 4092 / 01 (2 Oct. 2001).

[49] LG Düsseldorf, 151 II 1/01 (29 Oct. 2001).

[50] OLG Düsseldorf, 3 Wx 351 / 01 (8 Feb. 2002).

[51] *Id.*

[52] VG Mainz, 1 L 1106101.MZ (19 Feb. 2002).

[53] *Id.* at 8.

4. The *Landgericht* Wiesbaden, the *OLG* Frankfurt and the *Landgericht* Berlin have denied the existence of an actual peril.[54] They say that the reasons for the application are only based on speculations and assumptions and add that even the Federal Government has repeatedly pointed out that there are no clues for terrorist attacks in Germany; however, the mere possibility of a terrorist attack is insufficient to create an actual peril.

5. The above observation has to be agreed to.[55] With good reason, the Landgericht Wiesbaden, at first, refers to the fact that the state legislator on purpose has made data screening dependent on an increased extent of danger, specifically because it is a mass intrusion into basic rights.[56] Here, the existence of an actual peril unreservedly has to be reviewed by the courts; they are not allowed to confine themselves to a control of mere plausibility.[57] This is due to the fact that in those federal states where a retention of the judge exists the court acts as the ordering instance, not as a supervising judge. In those federal states the police authorities only enter an application, the intrusion into basic rights is directed by the court alone.

The applications for data screening directed by the police could not present concrete clues, based on facts, that the life or physical condition of the people of Germany were in danger. The possibility to become a victim of a terrorist attack cannot be completely ruled out for any person, at any time, at any place in the world. However, this is not sufficient to claim the existence of an actual danger, to do so would completely deprive this predicate of any restrictive effect and attach the mere function as an alibi to it. Therefore, legal literature cites as examples of actual danger, states of emergency, and other similar situations, those situations where there is the kidnapping of an individual by terrorists or a probable threat of kidnapping.[58] Evidently, there is no comparable danger, proven by concrete facts, for an domestic German subject of protection.

The danger of terrorist attacks in foreign countries are not – in contrast to the opinion of the

---

[54] LG Wiesbaden, 4 T 707/01, 3 (6 Feb. 2002); LG Berlin, 84 T 8 / 02 (15 Jan. 2002); OLG Frankfurt, 20 W 55/02 (21 Feb. 2002).

[55] *See also* Welp, *quoted in* UNICUM No. 11 (2001), at 18; Gössner, FRANKFURTER RUNDSCHAU, (No. 85) 12 Apr. 2002, at 7.

[56] LG Wiesbaden, 4 T 707/01, p. 3 (6 Feb. 2002).

[57] OLG Frankfurt, 20 W 479 / 01, (8 Jan. 2002); OLG Frankfurt, 20 W 55/02, 4 (21 Feb. 2002); BVerfG, 83, 24.

[58] Tegtmeyer, PolG NRW, 8th edition, § 31, annotation 6.

Verwaltungsgericht Mainz[59] – a strong basis for intrusions into basic rights carried out by the police, since the police are not competent to fight against such a danger. Apparently, such a competence does not result from the state's duty to protect life and the realization of human rights – as the court believes. The mere fact that fundamental principles like these are considered for questions of competence should arouse a distrust of this argumentation.

Furthermore, such a duty to protect only relates to domestic inland subjects of protection and to dangers which present in Germany. Therefore, no one will assert that the police of Rheinland-Pfalz – referring to the German *Grundgesetz* (Basic Law), which demands the protection of life – are competent and authorized to conduct investigations in the USA in order to prevent attacks on American cities. Just as little, a danger for foreign subjects of protection which could realize in a foreign country, entitles the police to inland investigations, because such a peril is out of the competence of the German police. The same is applicable to the reference to the competence of the state police concerning the prosecution of crime by the *Verwaltungsgericht* Mainz. In an inadmissible way the court mixes the conditions for repressive and preventive acting, when it wants to deduce the competence of the police of Rheinland-Pfalz for *preventing* crimes from § 6 StGB. The authorities, mainly the public prosecutor's offices, can act repressively, if one of the crimes mentioned in § 6 StGB is suspected to exist, even if this crime has been committed in a foreign country.

This does not necessarily mean that the police are competent to conduct *preventive* investigations, as soon as anywhere in the world anybody is planning to deal with narcotics (§ 6 No. 5 StGB). On the contrary, state police only becomes competent, if either subjects of protection of the federal state or those of its citizens are endangered or if the possibility of danger within the federal state exists. Both the situations do not apply to the fear of further attacks in a foreign country. The same analysis fits the situation where German citizens were injured in the attacks on 11 September 2001, which according to § 7 StGB – as the *Verwaltungsgericht* Mainz points out – brings into application German criminal law, as well. In this case the court also mixes repressive and preventive acting in an inadmissible way. Because German citizens were injured in the attack in New York, it was possible for public German authorities to act repressively on the basis of § 98 a StPO in order to clear up that crime. To become competent for a prevention of crime in foreign countries concrete clues are necessary that showing German subjects of protection are in danger again. Currently, this cannot be assumed without getting absorbed in

[59] VG Mainz, 1 L1106101.MZ, 9 (19 Feb. 2002).

speculations. The mere fear that German citizens could be injured in attacks anywhere in the world does not prove an actual danger according to police law.[60]

The point that required certainty of damage decreases as the extent of the possible damage increases is unconvincing in this situation.[61] Anyhow, the state legislators have permitted data screening only if extremely essential subjects of protection (physical condition, life, freedom, the survival or safety of the Federal Government or of a federal state) are endangered. In spite of the high importance of these subjects of protection not just any danger is sufficient for the state legislator to allow data screening, but they demand the existence of an actual danger to do so. Consequently, if one wants to decrease the demands on the probability of danger with reference to the high importance of the endangered subjects of protection, one disregards the evident intention of the legislator. The substitution of the predicate "actual danger" by terms like "urgent danger," or "concrete danger," which demand lower degrees of danger, are actions exclusively reserved for the legislator, as the OLG Frankfurt points out with full justification.[62] The terrorist attacks which brought about data screening were only directed against the United States. At no time in the past was there a threat to life and physical condition in the German federal states, and concrete circumstances (in contrast to mere fear) which could prove such dangers in the future are totally missing.

If – as the OLG Düsseldorf believes – different public institutions were striking, potential aims of terrorist attacks,[63] the question must be asked, why the nuclear power stations, for instance, are not deactivated, because they are apparently regarded as potential aims. For such safety precautions the danger apparently was not actual enough.[64]Rightly, the *Landgericht* Berlin and the *Landgericht* Wiesbaden refer to press releases of the Federal Government (e. g. from 10 October 2001), which say that the Federal Ministry of the Interior, even after the attacks on targets in Afghanistan, has no clues of intended terrorist attacks in Germany.
On 20 September 2001, the Federal Government declared that there was no actual danger for Germany. On 26 September 2001, another press release of the Federal Government pointed out that the Ministry of the Interior as well as the secret services had discovered no reason for concern at the moment. On the contrary, they

---

[60] OLG Frankfurt, 20 W 55/02, 7 (21 Feb. 2002).

[61] *Id.*.

[62] *Id.*

[63] OLG Düsseldorf, 3 Wx 357/01, 3 (8 Feb. 200).

[64] FRANKFURTER RUNDSCHAU, (No. 35) 11 Feb. 2002, at 3; Gössner, FRANKFURTER RUNDSCHAU, (No. 85) 12 Apr. 2002, at 7.

mentioned "eventualities", which hopefully would not happen. Consequently, if even the Ministry of the Interior on the basis of its secret service sources arrives at the conclusion that there is no actual danger for German subjects of protection, then the judgement of the *Landgericht* Düsseldorf that there is an actual danger for the survival or the safety of the Federal Government or a federal state cannot prevail: The highest representatives of this subject of protection have publicly declared the opposite.

III. The proportionality of intrusion

The considerable importance of data screening as a mass intrusion into basic rights demands an especially careful examination of proportionality in the individual case.[65]

1. Suitability

Mainly, there are doubts about the fulfilment of the principles of proportionality in connection with the partial principle of suitability to repel dangers which could come from the members of the terrorist organisation around Bin Laden.[66] The search criteria which data screening is based on are by far too general to result in the group of foreign students they are directed to find.[67] For instance, in Nordrhein-Westfalen about 11,000 cases were left to investigate when data screening was finished (and circa 2.000 persons in Bavaria).[68]

These result again demonstrates that data screening is an unqualified means of discovering persons, whose characteristic feature is inconspicuousness. This thesis is proved by the processes' complete ineffectiveness, which was revealed in spring 2002.[69] Therefore, data screening would only have been suitable to repel perils, if there had been at least one criterion that could have been a concrete indication of a potential terrorist plot. However, the data screenings take into account as a search criteria the very circumstance that a person has not become conspicuous to the police.

---

[65] OLG Düsseldorf, 3 Wx 357/01, 7 (8 Feb. 2002).

[66] OLG Frankfurt, 20 W 55 / 02, 8 (21 Feb. 2002). "material doubts."

[67] Welp, *supra* note 55; Jansen, FRANKFURTER RUNDSCHAU, (No. 40) 16 Feb. 2002, at 5.

[68] FRANKFURTER RUNDSCHAU, (No. 40) 16 Feb. 2002, at 5; WESTFÄLISCHE NACHRICHTEN, (No. 31) 6 Feb. 2002, at RMS 1.

[69] FRANKFURTER RUNDSCHAU, (No. 35) 11 Feb. 2002, at 1.

2. Necessity

It is also doubtful of the necessity for, as in Nordrhein-Westfalen for example, universities to hand over the data of German citizens to the police. Rightly, the OLG Düsseldorf has declared data screening disproportional,[70] because German citizens who are not members of the Islamist community , are not even theoretically assumed to become terrorists.[71] As data screening results in other federal states show, the restriction of the method on citizens of certain countries and on Islamist believers is an equally suitable, but more gentle means, compared with the inclusion of the entire male population.

3. Appropriateness

Therefore, data screening would only be proportional concerning foreign citizens and Islamist believers. As a matter of fact, these data are the only remaining search criteria besides age and sex. Finally, there is no selection of a group of people with certain criteria from the unmanageable amount of the entire population with the help of concrete search criteria, as it would correspond to the conception of data screening. Instead, large groups of the population are imputed a kind of affinity to danger – a finding which amounts to a general suspicion. Consequently, this kind of data screening is hardly suitable to discover potential terrorists, but instead supports prejudices – spread within the entire population – against certain groups of the population.[72]

F. Data screening on the basis of the criminal procedure code

Since there was no present danger for subjects of protection in Germany, the question arises why the police did not base their proceeding on § 98 a StPO, which does not contain this pre-condition. Data screening can be based both on police law and on criminal procedure law ("double-functional method."[73]) The cause of such a proceeding could have been the suspicion of the existence of a terrorist organisation.

---

[70] OLG Düsseldorf, 3 Wx 357 / 01 (8 Feb 2002).

[71] *Id.*

[72] FRANKFURTER RUNDSCHAU, (No. 37) 13 Feb. 2002, at 3.

[73] Lisken & Denninger, *supra* note 45, at chapter E, annotation 155; Tegtmeyer, PolG NRW, § 1, annotation 39.

§ 98 a StPO requires a suspect with regard to one of the offences that are numerated in the first paragraph. According to § 98 a (1), No. 2 StPO, in conjunction with § 120 (1) No. 6 of the constitution of the courts-code ("Gerichtsverfassungsgesetz" – "GVG"), the suspicion of the existence of a terrorist organisation (§ 129 a StGB) is sufficient. On the other hand § 129 a StGB requires that the organisation possesses at least an independent sub-organisation in the F.R.G.[74] Such independent structures of the Al-Quaeda-network did not exist in Germany (unlike the Kurdish "PKK," for example). Therefore, a suspicion sufficient for § 98 a StPO did not exist at that time (the new § 129 b StGB which extends the scope of application of § 129 a StGB on foreign terrorist organisations could not have been applied[75]).

G. Right to restitution

Unsolved is the question of how to deal with the all the collected personal data. According to the state laws the data must be deleted as soon as they cease to be used.[76] For example, in Nordrhein-Westfalen disks with the data of about 5 million men were destroyed publicly in a waste incineration plant.[77]

But the question arises what happens with the data of those persons to whom the extremely abstract criteria apply (so called "Recherchefälle"[78]). This regards to the data of 11,000 persons in Nordrhein-Westfalen solely. After the terrorist attacks in September 2001, the Federal Bureau of Criminal Investigation ("Bundeskriminalamt") created a data file called "Verbunddatei Schläfer" where all state police agencies transmit their information.[79] Therefore, the data of tens of thousands law abiding persons could be preserved at the Federal Bureau of Criminal investigation. A similar data collection happened in connection with the terrorist investigation in the seventies. At that time the Federal Bureau of Criminal Investigation created a data file called "PIOS" (persons, institutions, objects and properties) where information concerning above 135,000 persons, 5,500 institutions, 115,000 objects and

---

[74] BGH 30, 329; Tröndle & Fischer, StGB, 50th edition, § 129 a, annotation 3, *in conjunction with* § 129, annotation 2.

[75] Draft: BT-Dr. 14 / 7025, 4 Oct. 2001; adopted by the Bundestag on 26 Apr. 2002.

[76] *E.g.* § 31 (3), 1 PolG NRW.

[77] WESTFÄLISCHE NACHRICHTEN, (No. 31) 6 Feb. 2002, at RMS 1.

[78] FRANKFURTER RUNDSCHAU, (No. 40) 16 Feb. 2002, at 5.

[79] FRANKFURTER RUNDSCHAU, (No. 35) 11 Feb. 2002, at 1.

more than 74,000 things were archived.[80] Amongst the registered persons were – inter alia – schoolmates, siblings and parents of suspects as well as the data of about 7,000 persons who had visited a suspect in prison. Only a few of these data files have been erased.[81] Therefore, there is reason to raise the question of what will happen with the collected data provided by all federal states. According to the interpretation of law argued here, the people who were targeted by data screening have the right of restitution that is aimed at deletion of their data from all data files of the state bureaus of criminal investigation and the Federal Bureau of Criminal Investigation.

H. Conclusion

I. The use of data screening as mass intrusion into the basic right of self-determination about personal data that identifies an indetermined multitude of unsuspicious persons requires a statutory regulation that restricts the screening to cases of an increased degree of danger and to dangers to important subjects of protection. Therefore, the statutory sources in police law conform with the principle of proportionality only as far as they require a present danger to life, physical integrity or personal freedom or to the integrity of the F.R.G. or a federal state.

II. The effective protection of basic rights through process requires prior control of the legal predicates by an independent judge (not the chief officer or the home secretary). For reasons of appropriate allocation of rights and duties and for reasons of efficiency of the judicial order as a protection-mechanism for basic rights, this control should be assigned to the administrative courts, not the regular courts.

III. By failing the predicate of a present danger for domestic subjects of protection the requirements of data screening for retrieval of Islamist terrorists were not complied with. Great intrusion into the right to data privacy of a multitude of unsuspicious persons constitutes a disproportional invasion of the right to self determination concerning personal data because it is an inappropriate method for tracing persons who are characterised by their inconspicuousness. So long as the personal data of persons to whom the extremely abstract criteria apply are recorded, these persons have a right of restitution which contains a claim for deletion of their data from the files of the bureaus of criminal investigation.

---

[80] AUST, DER BAADER-MEINHOF-KOMPLEX 203 (Berlin 1989).

[81] *Id.* at 203-4.