www.jusletter-it.eu

Sandra Husi-Stämpfli

Die Technik galoppiert voran – wo bleibt das Recht?

Technische Hilfsmittel halten Einzug in den Verwaltungsalltag

Technology increasingly takes over control of the administrative life. What challenges need to be faced from a legal point of view, especially considering data protection and information security? Can everything remain as it is? Are there required amendments in legal bases respectively in organisational structures? The author focuses on these questions and shows that solution approaches must not only be of legal nature: A rethinking regarding assuming responsibility within the administration must happen as well as a serious conception and realisation of a cantonal IT-Governance. (ah)

Category: Scientific Articles
Region: Switzerland
Field of law: Data Protection; IT-Governance

Citation: Sandra Husi-Stämpfli, Die Technik galoppiert voran – wo bleibt das Recht?, in: Jusletter IT 24 September 2015

Inhaltsübersicht

I. Die Technik hält Einzug in den Verwaltungsalltag

[Rz 1] Lehnen Sie sich doch einmal in Ihrem Bürostuhl zurück und versuchen Sie sich vorzustellen, wie ihr Verwaltungsalltag ohne technische Hilfsmittel aussehen würde. Um nur ein paar Szenarien aufzuzeigen: Anstelle des PCs hätten Sie eine Schreibmaschine – zwar aus heutiger Sicht nicht sonderlich praktisch, aber immerhin müssten Sie Ihre Briefe nicht von Hand schreiben. Anrufbeantworter und Anzeige verpasster Anrufe auf dem Telefon? Kann ein Anruf nicht entgegen genommen werden, muss eben ein weiteres Mal angerufen werden. Datenbank der aktuellen Geschäfte? Karteikarten, Papierakten, Internet-Recherche bzw. internetbasierte Archive? Alles auf Papier, in Lexika, die von Menschenhand und -auge durchsucht werden müssen. Online-Kalender mit Übersicht über alle Teammitglieder und deren Termine? Ein Anschlagsbrett im Gang des Büros gibt ebenso Auskunft über An- und Abwesenheiten. Und schliesslich: Erreichbarkeit rund um die Uhr, Zugriff auf die laufenden Geschäfte und Abrufen der eingegangenen Mails via Smartphone und entsprechenden Apps? Von wegen – was während der Arbeitszeit nicht erledigt werden konnte, muss entweder in Papierform nach Hause mitgenommen werden, oder wartet eben bis zum nächsten Tag.

[Rz 2] Aber nicht nur im Büro übernimmt die Technik das Steuer. So greifen beispielsweise auch Blaulichtorganisationen immer mehr auf neue technische Errungenschaften zurück: Von der Ab-

schnittsgeschwindigkeitskontrolle[1], Drohnen[2] und eigenen Kommunikations-Apps[3] über Apps, welche die Gesundheitsdaten eines Patienten auf dessen Handy verwalten und im Notfall zugänglich machen[4]: Wir nutzen bei der Erfüllung unserer Verwaltungsaufgaben je länger je mehr technisch hochentwickelte Geräte und können uns den Verwaltungsalltag ohne diese «Gadgets» schon fast nicht mehr vorstellen – obwohl die Zeit vor der technischen Revolution noch nicht allzu weit zurück liegt.

[Rz 3] Die Technik galoppiert bereits heute forsch voran – und dabei stehen wir, will man den Entwicklern glauben[5], erst am Anfang dieser Entwicklung. Die technischen Hilfsmittel werden immer gewiefter, intelligenter, können uns immer mehr Aufgaben abnehmen, ermöglichen uns immer mehr. Was früher selbstverständlich von Menschen erledigt wurde, wird heute von Applikationen übernommen – sei dies das Durchsuchen der Geschäftsablage oder das Bestellen des Kaffeenachschubs (intelligente Kaffeemaschinen in Grossraumbüros lösen heutzutage Kapsel-Bestellungen beim Händler aus).

[Rz 4] Wo bleibt bei diesem rasanten Entwicklungs-Galopp aber der rechtliche Rahmen? Wenn seit langem eingespielte Verwaltungsaufgaben plötzlich mit technischen Hilfsmitteln oder gar vollautomatisiert erfüllt werden – genügen die bestehenden gesetzlichen Grundlagen noch? Dem Datenschutzbeauftragten des Kantons Basel-Stadt wurde auf diese Frage hin regelmässig entgegnet: «Wir machen ja das gleiche wie bis anhin, einfach mit anderen Mitteln.» Muss also davon ausgegangen werden, dass ein (allenfalls seit mehreren Jahrzehnten bestehendes) Gesetz, welches eine öffentliche Aufgabe nennt, diese bezüglich der einsetzbaren Mittel neutral umschreibt?

[Rz 5] Der folgende Beitrag geht dieser Frage nach: In einem ersten Teil sollen die rechtlichen Rahmenbedingungen für den Einsatz von «Technik» im Verwaltungsalltag[6] beleuchtet werden. Der zweite Teil illustriert die Problematik anhand von drei Beispielen und zeigt auf, welche Überlegungen es anzustellen gilt, wenn der technische Fortschritt Verwaltungsabläufe vereinfachen soll. Im dritten und letzten Teil sollen schliesslich allgemeine Lösungsansätze erarbeitet und vorgestellt werden, so dass die Technik dem rechtlichen Rahmen künftig nicht mehr davongaloppieren kann.

II. Flickwerk rechtlicher Rahmen

[Rz 6] Das Abstecken des rechtlichen Rahmens für den Einsatz technischer Geräte bzw. Hilfsmittel im Verwaltungsalltag gestaltet sich reichlich schwierig: Berücksichtigt werden müssen zum einen die allgemeinen Vorgaben des Datenschutzrechts, wenn mit den technischen Geräten Personendaten bearbeitet werden. Die Informationssicherheit – welche nicht mit «dem Datenschutz» zu verwechseln ist – wird teilweise ausgesprochen stiefmütterlich behandelt, muss aber eine wesentliche Rolle

1 http://www.astra.admin.ch/00638/?lang=de&msg-id=43400 (alle Internetquellen zuletzt besucht am 31. Juli 2015).

2 http://www.srf.ch/news/schweiz/noch-luft-nach-oben-nur-drei-polizeikorps-setzen-auf-drohnen.

3 http://www.netzwoche.ch/de-CH/News/2015/04/30/Abraxas-erhaelt-Zuschlag-fuer-Polizei-Whatsapp.aspx.

4 http://www.express.de/digital/20-notfall-apps-so-wird-das-iphone-zum-lebensretter,2492,7507694.html.

5 http://www.verivox.de/nachrichten/vernetzter-alltag-immer-mehr-intelligente-geraete-104267.aspx.

6 Es würde den Rahmen dieses Beitrags sprengen, wenn auch der Einzug der intelligenten Geräte in unseren privaten Alltag diskutiert würde: In diesem Themenbereich bearbeiten Private Personendaten, entsprechend andere rechtliche Vorgaben gilt es zu beachten. Zu den Herausforderungen, welche sich mit dem Einsatz intelligenter Haushaltsgeräte für die informationelle Selbstbestimmung ergeben, siehe Sandra Husi-Stämpfli, Wenn der Backofen mit dem Staubsauger kommuniziert…, in: Jusletter IT 11. Dezember 2014.

spielen. Schliesslich muss auch bereichsspezifisches Recht, welches die konkrete Aufgabenerfüllung regelt, berücksichtigt werden, obschon dieses meistens deutlich hinter der technischen Entwicklung hinterher hinkt – so stammt beispielsweise das baselstädtische Schulgesetz aus dem Jahr 1929[7], also einer Zeit, in welcher an Schulhomepages, elektronische Schülerakten und E-Mail Kommunikation noch nicht einmal gedacht wurde.

1. Datenschutzrechtliche Vorgaben und Informationssicherheit

1.1. Datenschutzrecht

[Rz 7] Datenschutzrechtliche Vorgaben sind von einer Verwaltungseinheit immer dann zu befolgen, wenn zur Erfüllung der jeweiligen Aufgabe Personendaten, d.h. Informationen, die die Identifikation einer konkreten Person erlauben, bearbeitet werden müssen. Für öffentliche Organe der Kantone gelten dabei die Regeln der jeweiligen kantonalen (Informations- und) Datenschutzgesetze, für Bundesorgane das Datenschutzgesetz des Bundes (DSG)[8].

[Rz 8] Ein Blick in die verschiedenen Datenschutzgesetze macht aber schnell deutlich, dass dort keine konkreten Vorgaben für den Einsatz technischer Hilfsmittel im Verwaltungsalltag erwartet werden können. Vielmehr finden sich in den Datenschutzgesetzen die allgemeinen Grundsätze des Datenbearbeitens, das sog. formelle Datenschutzrecht[9]: Sie enthalten die Datenschutzgrundsätze (insb. Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung, Richtigkeit, Erkennbarkeit der Beschaffung und/oder Informationspflicht[10]), legen die Verantwortung des datenbearbeitenden öffentlichen Organs fest[11] und formulieren die Voraussetzungen, unter welchen das Datenbearbeiten[12] und, als Unterkategorie, das Datenbekanntgeben zulässig sind[13]. Dabei legen sie auch fest, wie die qualifizierten Voraussetzungen für das Bearbeiten und Bekanntgeben von besonders schützenswerten (oder besonderen) Personendaten aussehen[14]. Sie enthalten Bestimmungen für das grenzüberschreitende Bekanntgeben von Personendaten[15] und privilegieren i.d.R. das Datenbearbeiten und -bekanntgeben zu nicht personenbezogenen Zwecken (wie Statistik, Planung und Forschung[16]). Häufig regeln sie auch das Bearbeitenlassen von Personendaten durch Dritte (Datenbearbeiten im

---

7 Schulgesetz des Kantons Basel-Stadt vom 4. April 1929, SG 410.100.

8 Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG, SR 235.1)

9 Siehe dazu ausführlich Beat Rudin, Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ 2009, 1 ff., krit. zum Begriff Thomas Gächter/Philipp Egli, Informationsaustausch im Umfeld der Sozialhilfe, in: Jusletter 6. September 2010, 43.

10 Z.B. Art. 4, 5 und 7 DSG, §§ 9 und 12 des Gesetzes des Kantons Zürich vom 12. Februar 2007 über die Information und den Datenschutz (LS 170.4, im Folgenden zitiert als IDG-ZH), §§ 9, 11, 12, 15 und 16 des baselstädtischen Gesetzes vom 9. Juni 2010 über die Information und den Datenschutz (SG 153.260, im Folgenden zitiert als IDG-BS).

11 Z.B. Art. 16 DSG; § 6 IDG-BS; Art. 6 des Schaffhauser Gesetzes vom 7. März 1994 über den Schutz von Personendaten (SHR 174.100).

12 Z.B. Art. 17 DSG, § 8 IDG-ZH, § 9 IDG-BS.

13 Z.B. Art. 19 DSG, § 16 IDG-ZH, § 21 IDG-BS.

14 Z.B. Art. 17 Abs. 2 und Art. 19 Abs. 1 DSG; § 8 Abs. 2 und § 17 IDG-ZH; § 9 Abs. 2 und § 21 Abs. 2 IDG-BS; § 9 Abs. 2 und § 19 des basellandschaftlichen Gesetzes vom 10. Februar 2011 über die Information und den Datenschutz (SG 162, im Folgenden: IDG-BL).

15 Z.B. Art. 6 DSG; § 19 IDG-ZH; § 23 IDG-BS; Art. 39 des Genfer loi du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (RSG A2 08)

16 Z.B. Art. 22 DSG; § 9 Abs. 2 und § 18 IDG-ZH; § 10 und § 22 IDG-BS; Art. 7 des St. Galler Datenschutzgesetzes vom 20. Januar 2009 (SG 142.1).

Auftrag, Outsourcing[17]) und die Pflicht, bestimmte Datenbearbeitungen einer Vorabkontrolle zu unterziehen[18]. Ausserdem räumen sie der betroffenen Person Rechte ein: das Recht auf Auskunft und Einsicht[19], auf Berichtigung unrichtiger Daten, auf Unterlassung, auf Beseitigung der Folgen des widerrechtlichen Bearbeitens und auf Feststellung der Widerrechtlichkeit eines Bearbeitens[20]. Und schliesslich regeln die Gesetze die Datenschutzaufsicht[21].

[Rz 9] Für die Beurteilung des Einsatzes technischer Hilfsmittel durch Verwaltungsbehörden helfen diese Grundsätze freilich nur bedingt – das Datenschutzrecht ist, von den noch aus den Anfängen des Datenschutzrechts stammenden Hinweisen auf «automatisierte Datenbearbeitungen» abgesehen, bislang weitestgehend technikneutral formuliert. Dies hat zwar den Vorteil, dass die Grundsätze eben als solche Bestand haben und nicht dem technischen Fortschritt unterworfen sind. Gleichwohl bleibt damit die Frage offen, ob die bisher bestehenden gesetzlichen Grundlagen bei der Einführung einer neuen Applikation oder ein neues Arbeitsinstrument genügen oder ob nicht allenfalls doch die dazu verwendeten Mittel mitberücksichtigt und die rechtlichen Grundlagen angepasst werden müssen.

[Rz 10] Um nochmals auf das Eingangs geschilderte Argument «wir machen das gleiche wie bisher, einfach mit einem neuen Instrument» zurückzukommen: Die geltenden Archivgesetze erlauben natürlich den Zugang zu den Archivalien und führen bestimmte Kriterien für die Zugangsgewährung auf. Können diese archivrechtlichen Bestimmungen aber 1:1 übernommen werden, wenn ein digitaler Lesesaal eingerichtet wird? Können die Publizitätsvorgaben des Schuldbetreibungs- und Konkursrechts – welches immerhin aus dem Jahr 1889 stammt – tel quel übernommen werden, wenn anstelle eines gedruckten Amtsblattes und eines Anschlags am Rathaus neu eine online Version des Amtsblattes publiziert werden soll? Oder ist es wirklich einerlei, ob säumige Fahrzeugsteuer-Zahlerinnen und -Zahler mittels ausgedruckten Excel-Tabellen auf der Strasse von Hand bzw. «von Auge» ermittelt, oder ob diese Tabellen in ein Nummernschild-Erkennungssystem in einem Polizeifahrzeug eingespiesen und beim Durchkreuzen der Quartiere abgeglichen werden?

[Rz 11] Dass diese Fragen allein gestützt auf die *Grundsätze* des Datenbearbeitens offen bleiben *müssen*, ist konsequent richtig. Gleichwohl darf dieses formelle Datenschutzrecht nicht ausser Acht gelassen werden, wenn der Einsatz technischer Hilfsmittel geprüft wird: Auch wenn neue Speichermöglichkeiten es erlauben, weitaus grössere Datensätze aufzubewahren, als es bislang mit Papierdossiers opportun erschien: Der Grundsatz der Verhältnismässigkeit verlangt auch bei digitalen Dossiers, dass nur jene Daten gespeichert werden, die für die Aufgabenerfüllung erforderlich sind, und auch mit dem Einsatz von digitalen Geschäftsablagen muss es möglich sein, Dossiers «zu schliessen» bzw. zu archivieren oder zu löschen.

[Rz 12] Das Datenschutzrecht bleibt damit seiner Rolle als Grundsatzrecht auch in Anbetracht der technischen Revolution treu (ja *muss* dieser Rolle treu *bleiben*) und ist entsprechend zu würdigen – wie bis anhin nicht als konkret fallbezogene Handlungsanweisung, sondern als Leitplanke, entlang

17 Z.B. Art. 10a DSG; § 6 IDG-ZH; § 7 IDG-BS oder auch § 17 des Solothurner Informations- und Datenschutzgesetzes vom 21. Februar 2001 (InfoDG, SG 114.1).

18 Z.B. § 10 IDG-ZH; § 13 IDG-BS, oder aber § 12 IDG-BL, nicht jedoch der Bund.

19 Z.B. Art. 8 DSG; § 20 Abs. 2 IDG-ZH; § 26 IDG-BS, samt den Voraussetzungen für die Einschränkung dieses Rechts, z.B. Art. 9 und Art. 10 DSG; § 23 IDG-ZH; § 29 IDG-BS.

20 Z.B. Art. 25 Abs. 1 und 3 DSG; § 21 IDG-ZH; § 27 IDG-BS; § 26 ff. InfoDG oder aber Art. 22 ff. des Tessiner legge del 9 marzo 1987 sulla protezione dei dati personali (RL 1.6.1.1).

21 Z.B. Art. 26 ff. DSG; § 30 ff. IDG-ZH; § 37 ff. IDG-BS oder § 18 des Zuger Datenschutzgesetzes vom 28. September 2000 (SG 157.1).

derer es sich zu bewegen gilt.

1.2. Informationssicherheit

[Rz 13] Dass Handlungs- bzw. Regelungsbedarf bezüglich des Einsatzes technischer Hilfsmittel beim Bearbeiten von Personendaten besteht, zeigen die neueren Datenschutzgesetze. Sie enthalten immerhin Grundsatzbestimmungen zur Informationssicherheit. Das IDG-BS hält beispielsweise fest, dass das öffentliche Organ seine Informationen durch angemessene organisatorische und technische Massnahmen schützen muss, wobei die folgenden Schutzziele zu berücksichtigen sind: Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit. Ähnliche Bestimmungen finden sich beispielsweise in den (Informations- und) Datenschutzgesetzen der Kantone Zürich[22], Luzern[23], Uri[24] oder Waadt[25].

[Rz 14] Auch das Datenschutzgesetz des Bundes verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 DSG)[26]. Die Art. 8 bis 10 sowie 20 und 21 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG)[27] konkretisieren die zum Schutz der Informationen vorzukehrenden Massnahmen. Insbesondere sind die Systeme zu schützen gegen unbefugte oder zufällige Vernichtung, zufälligen Verlust, technische Fehler, Fälschung, Diebstahl oder widerrechtliche Verwendung, unbefugtes Ändern, Kopieren, Zugreifen und andere unbefugte Bearbeitungen (Art. 8 Abs. 1 VDSG). Das verantwortliche Bundesorgan muss ein Bearbeitungsreglement erstellen für automatisierte Datensammlungen, die (alternativ) a) besonders schützenswerte Daten oder Persönlichkeitsprofile beinhalten, b) durch mehrere Bundesorgane benutzt werden, c) Kantonen, ausländischen Behörden, internationalen Organisationen oder privaten Personen zugänglich gemacht werden; oder d) mit anderen Datensammlungen verknüpft sind (Art. 21 Abs. 1 lit. a–d VDSG).

[Rz 15] In diesem Bearbeitungsreglement legt das verantwortliche Bundesorgan seine interne Organisation fest[28]. Dieses umschreibt insbesondere die Datenbearbeitungs- und Kontrollverfahren und enthält alle Unterlagen über die Planung, Realisierung und den Betrieb der Datensammlung.

[Rz 16] Für den Einsatz neuer Technologien bzw. neuer technischer Hilfsmittel sind diese Vorgaben insofern essentiell, als dass sie die Risiken, die durch die neuen Technologien für die bearbeiteten

---

22 § 7 IDG/ZH.

23 § 7 des Luzerner Gesetzes vom 2. Juli 1990 über den Schutz von Personendaten (SRL 38).

24 Art. 11 des Urner Gesetzes vom 20. Februar 1994 über den Schutz von Personendaten (RB 2.2511), wobei der Wortlaut sehr knapp gehalten ist.

25 Art. 10 des Waadtländer loi du 11 septembre 2007 sur la protection des données personnelles (RSV 172.65) mit ebenfalls sehr knappem Wortlaut.

26 Vgl. dazu David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 7 N 2 ff.; Astrid Epiney, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht, Bern 2011, § 9 Rz. 50 ff.; Philippe Meier, Protection des données, Bern 2010, Rz. 780 ff.; Christa Stamm-Pfister, Art. 7 Rz. 7 ff., in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar zum Datenschutzgesetz, 3. Auflage, Basel 2014 (im Folgenden zitiert als BSK-DSG-AutorIn); zum kantonalen Recht: Bruno Baeriswyl, § 8 N 9ff., in: Beat Rudin/Bruno Baeriswyl (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt, Zürich 2014 (im Folgenden zitiert als PK-IDG/BS-AutorIn); Bruno Baeriswyl, § 7 N 7 ff., in: Bruno Baeriswyl/Beat Rudin (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich, Zürich 2012 (im Folgenden zitiert als PK-IDG/ZH-AutorIn)

27 Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11).

28 Dazu Rosenthal/Jöhri (Fn 26), Art. 7 Rz. 22 ff.; Epiney, in: Belser/Epiney/Waldmann (Fn 26), § 9 Rz. 57; Meier (Fn 26), Rz. 815 ff.; BSK-DSG-Stamm, Art. 7 Rz. 53.

Personendaten zu minimieren suchen, und die jeweiligen Amtsstellen bzw. unter Umständen gar ganze Departemente[29] anhalten, Informationssicherheitskonzepte zu erstellen und die Verantwortung für den Einsatz der neuen Technologien zu übernehmen. Damit soll zumindest der teilweise noch immer sehr naiv anmutende Umgang mit neuen Technologien in geordnete Bahnen gelenkt werden: Nur weil beispielsweise Google Analytics ausgesprochen praktisch erscheint, um das Besucherverhalten auf kantonalen Webseiten zu beobachten und den eigenen Webauftritt entsprechend zu optimieren, nur weil es deutlich einfacher ist, die Anmeldung von neuen Bürgerinnen und Bürgern via sog. Online-Schalter abzuwickeln, heisst dies nicht, dass damit nicht auch grosse Risiken für die Persönlichkeitsrechte der betroffenen Personen verbunden sind.

[Rz 17] Auch diese Vorgaben können aber die Frage nach der grundsätzlichen Rechtmässigkeit des Einsatzes der neuen Technologien zur jeweiligen gesetzlichen Aufgabenerfüllung nicht beantworten. Es bleibt nur, den Blick auf das jeweilige Sachrecht zu richten.

2. Sachrecht

[Rz 18] Während das formelle Datenschutzrecht die Grundsätze des Datenbearbeitens festhält, ist dem sog. materiellen Datenschutzrecht, d.h. dem jeweiligen Sachrecht, zu entnehmen, zur Erfüllung welcher Aufgaben Personendaten von wem bearbeitet werden dürfen – und allenfalls auch, mit welchen Mitteln dies geschehen soll. Ein paar Beispiele: Die Sozialhilfe findet im Sozialhilfegesetz, welche Daten bei wem erhoben werden dürfen, um den tatsächlichen Sozialhilfebedarf einer Gesuchstellerin zu berechnen, wem diese Informationen weitergegeben werden können etc. Das kantonale Archiv gründet seine Tätigkeit auf das jeweilige Archivgesetz, welches beispielsweise Schutzfristen und Zugangsmodalitäten nennt. Die Aufgaben der Kantonspolizei sind im jeweiligen kantonalen Polizeigesetz enthalten, die Aufgaben der Schulbehörden und Lehrkräfte im kantonalen Schulgesetz, die Zuständigkeiten und die daraus resultierenden Datenbearbeitungsvorgänge der kantonalen IV-Stellen im IV-Gesetz des Bundes, usw.

[Rz 19] *Ob*, und wenn ja *welche*, technischen Hilfsmittel zur jeweiligen Aufgabenerfüllung beigezogen werden dürfen, und insbesondere auch *wie* sich dieser Einsatz zu gestalten hat, wird dabei aber nur sporadisch geregelt – auch das Sachrecht ist heute (noch) weitestgehend technikneutral formuliert. Für das Open System Invaliden-Versicherung (OSIV), d.h. die Geschäftskontrolle der Sozialhilfebehörden finden sich beispielsweise keine expliziten Rechtsgrundlagen, vielmehr wird der Einsatz dieses Systems als «zur Aufgabenerfüllung» erforderlich betrachtet und damit unter die entsprechenden Aufgabennormen der Sozialhilfe subsumiert; gleiches gilt für die Datenbanken der Schulen zur Schüler(innen)verwaltung, wobei diese Datenbanken je länger je mehr auch Informationen von schulaffilierten Diensten wie insbesondere der Schulsozialarbeit, dem Schulpsychologischen Dienst oder den Heilpädagogischen Diensten enthalten – und dabei längst nicht mehr reine Administrativdatenbanken sind. Und in den Archivgesetzen wiederum finden sich keine Bestimmungen darüber, ob der Zugang zu den Archivalien in analoger oder gar in digitaler Form gewährt werden kann. Dagegen werden die jeweiligen Informationssysteme, welche den Polizeibehörden zur Verfügung stehen, im Bundesgesetz über die polizeilichen Informationssysteme (BPI) reglementiert.

[Rz 20] Allein dieser «Kleinst-Überblick» zeigt, dass der Einsatz technischer Hilfsmittel bzw. die Digitalisierung der Verwaltung höchst unterschiedlich geregelt wird: Augenscheinlich ist dabei, dass

[29] Zur Verantwortung siehe in diesem Beitrag IV, Ziff. 2.

insbesondere ältere Gesetze noch keine Regelungen zum digitalisierten Verwaltungsalltag enthalten und daher der Einsatz von Informationssystemen grundsätzlich als «zur Aufgabenerfüllung erforderlich» und damit nicht besonders regelungsrelevant erachtet wird. Ebenso ist nachvollziehbar, dass Behörden wie die Kantonspolizei, welche mit ihrem Handeln schwerwiegend in die Grundrechte der betroffenen Personen eingreifen (können), über klare Vorgaben bezüglich der erlaubten Mittel verfügen.

[Rz 21] Nicht nachvollziehbar ist jedoch, weshalb die Gesetzgeber sich bislang zieren, bei den zahlreichen Revisionen der «alten» Gesetze (aber auch bei der Schaffung neuer Regelungen!) die Digitalisierung der Verwaltung zu thematisieren und dabei dem Umstand Rechnung zu tragen, dass mit dem Einsatz von digitalen Aktenablagen oder Informationssystemen das Risiko für Persönlichkeitsverletzungen erheblich steigt: Es können mehr Daten über längere Zeiträume hinweg aufbewahrt, leichter zugänglich gemacht und mit anderen Datenbanken verknüpft werden. Schliesslich ist die Informationssicherheit bei digitalen Systemen weitaus schwieriger zu gewährleisten wie bei Papierakten. Mit der bisherigen papier-basierten Verwaltungstätigkeit hat dies unzweifelhaft nur noch wenig Ähnlichkeiten, umso bedenklicher erscheint es daher, dass die bestehenden gesetzlichen Grundlagen ohne weitere Prüfung als «genügend» erachtet und in den Projektphasen regelmässig übergangen werden.

[Rz 22] Der folgende Abschnitt soll die hier skizzierte Problematik anhand von drei Beispielen weiter beleuchten und dabei der Frage nachgehen, ob es tatsächlich weitreichender Gesetzesrevisionen bedarf, oder ob allenfalls andere Massnahmen, wie die Erstellung von Informationssicherheitskonzepten etc., den Schutzanforderungen genügen könnten.

III. Schöne neue Verwaltungswelt

[Rz 23] Nicht nur die öffentliche Verwaltung erhofft sich von der technischen Revolution eine Vereinfachung von Arbeitsabläufen, auch die Erwartungshaltung der Bürgerinnen und Bürger verändert sich: Formulare sollen möglichst online abgerufen werden können, archivierte Unterlagen möglichst ebenfalls ohne einen Gang ins Staatsarchiv eingesehen werden, und da elektronische Zeitungen den klassischen Print-Ausgaben mittlerweile den Rang abgelaufen haben[30], soll bitteschön auch das Amtsblatt online publiziert werden.

[Rz 24] Wie den Bedürfnissen der Verwaltungsangestellten und der Öffentlichkeit nach möglichst optimalen Einsätzen der neuen Technologien Rechnung getragen werden soll, und ob bzw. in wieweit das Recht in diesen Bereichen «hinterher hinkt», illustrieren die folgenden drei Beispiele:

1. Das Online-Amtsblatt

1.1. Vom Anschlag zum Amtsblatt zur Online-Edition

[Rz 25] Das kantonale Amtsblatt (regelmässig auch Kantonsblatt genannt) dient der öffentlichen Verwaltung seit jeher als Publikationsorgan, wobei nicht nur neue Gesetze, Verordnungen und

30 Siehe dazu nur https://blog.opendatacity.de/der-zerfall-der-printmedien/> oder aberhttp://www.welt.de/welt_print/article3557695/Das-grosse-Zeitungssterben.html.

Beschlüsse[31] bekannt gemacht, sondern insbesondere auch zivilstandsrelevante Informationen wie Geburten, Todesfälle und Hochzeiten (bzw. früher noch Verlobungen)[32] publiziert und Betreibungsurkunden[33] und Strafurteile[34] veröffentlicht werden.

[Rz 26] Das «Anschlagen» dieser Informationen an besucherstarken Orten wie dem Marktplatz, dem Rathaus oder an Kirchplätzen wurde abgelöst vom gedruckten Amtsblatt – welches wiederum langsam aber sicher dem Online-Amtsblatt das Feld räumen muss. Dabei wird aber derzeit noch nicht völlig auf die Papier-Version verzichtet: Online-Amtsblatt und Printversion werden regelmässig parallel veröffentlicht, wobei einer Version die Verbindlichkeit zugesprochen wird.

1.2. Öffentlichkeit damals und heute: Herausforderungen

[Rz 27] Die Hintergründe für die Publikation von Informationen im Amtsblatt sind vielfältig, zielen aber allesamt letztendlich darauf ab, dass einem breiten Publikum bzw. daraus einzelnen Individuen die Möglichkeit zur Wahrung seiner/ihrer Rechte eingeräumt wird, oder dass sich einzelne Personen den Folgen ihres Handelns durch Verweigerung des amtlichen Schriftenverkehrs und der ordentlichen Zustellung nicht weiter entziehen können[35]. Mit dem technischen Fortschritt untrennbar verbunden ist natürlich auch der Wandel dieser Öffentlichkeitskonzeption.

[Rz 28] Während zu Zeiten des Anschlags des Amtsblatts an wichtigen Plätzen einer Stadt ein reichlich kleiner Kreis an Personen die Informationen zur Kenntnis nehmen konnte – nämlich jene, die diese Plätze zum richtigen Zeitpunkt frequentierten –, wurde mit der Printversion des Amtsblattes der Kreis potentieller Leserinnen und Leser deutlich erweitert. Der letzte Schritt, die Publikation im Internet, bringt nun eine gänzlich neue Dimension der Öffentlichkeit mit sich: Personen können nun weltweit gesucht und gefunden werden.

[Rz 29] Doch es ist nicht nur der «Kreis der Öffentlichkeit», der sich durch den technischen Fortschritt erheblich erweitert hat. Auch die Dauer der Zugänglichkeit hat sich verändert und stellt das ursprüngliche Konzept der Öffentlichkeit vor grosse Herausforderungen: Wurde früher ein Anschlag des Amtsblattes ausgewechselt, so musste doch immerhin ein Gang ins Rathaus oder später gar ins Archiv unternommen werden, um an Informationen über eine bestimmte Person zu gelangen. Gleiches galt für die Print-Versionen des Amtsblattes: Einmal im Altpapier entsorgt, konnte entweder eine neue Version bestellt oder eben im Rathaus bzw. im Archiv eingesehen werden. Sprich: Es mussten gezielte Anstrengungen unternommen werden, wenn über eine bestimmte Person Informationen über Schuldenrufe, Nachkommen oder Strafurteile in Erfahrung gebracht werden sollten. Zwar waren diese Informationen einst öffentlich gewesen und auch weiterhin grundsätzlich öffent-

---

31 Siehe dazu exemplarisch die baselstädtische Verordnung vom 3.Januar 1984 betreffend Publikation, Wirksamkeit und Aufhebung allgemeinverbindlicher Erlasse (Publikationsverordnung; SG 151.300) oder aber die Glarner Publikationsverordnung vom 12. August 2014 (GS I D/24/2).

32 Vgl. beispielsweise § 1 des baselstädtischen Gesetzes vom 27. April 1911 betreffend die Einführung des Schweizerischen Zivilgesetzbuches (SG 211.100) sowie Art. 10 des Jurassischen loi du 9 novembre 1978 sur les publications officielles (RSJU 170.51).

33 Art. 35 des Bundesgesetzes vom 11. April 1889 über Schuldbetreibung und Konkurs (SchKG, SR 281.1).

34 Art. 88 der Schweizerischen Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0) i.V.m. bspw. § 26 des baselstädtischen Gesetzes vom 13. Oktober 2010 über die Einführung der Schweizerischen Strafprozessordnung (SG 257.100).

35 Siehe dazu Francis Nordmann, Art. 35 N 1, in: Adrian Staehelin/Thomas Bauer/Daniel Staehelin (Hrsg), Kommentar zum Bundesgesetz über Schuldbetreibung und Konkurs, 2. Auflage, 2010 Basel oder aber Sarard Arquint, Art. 88 N 1 ff., in: Marcel Alexander Niggli/Marianne Heer/Hans Wiprächtiger, Basler Kommentar zur Schweizerischen Strafprozessordnung und zur Jugendstrafprozessordnung, 2. Auflage, 2014 Basel.

lich zugänglich, gleichwohl konnten die fraglichen Personen doch nicht ohne weiteres aufgespürt werden. Heute fördert jedoch eine einfache Anfrage bei einer Suchmaschine weit zurückliegende Informationen zu Tage – und spätestens, seit auch ehemals gedruckte Dokumente nachträglich digitalisiert und so im Internet zugänglich gemacht werden, sogar auch Informationen, die noch aus dem «analogen Zeitalter» stammen.

[Rz 30] Entspricht dies, insbesondere in puncto Bekanntgabe von Personendaten, noch der ursprünglichen Idee der Öffentlichkeit? Oder wurde bei der Konzeption der öffentlichen Bekanntmachung bzw. der Zustellungsfiktion davon ausgegangen, dass auch einmal öffentlich gemachte Informationen irgendwann in Vergessenheit geraten sollen, bzw. dass der Zugang zu diesen Informationen mit dem Lauf der Zeit deutlich schwerer werden soll?

[Rz 31] Betrachtet man den Zweck der Publikation von Bekanntmachungen des Betreibungs- und Konkursrechts und Strafurteilen, so wird schnell deutlich: Ab einem gewissen Zeitpunkt ist es nicht mehr erforderlich, dass ein Strafurteil ohne weiteres aufgefunden werden kann, und auch eine Bekanntmachung des Schuldbetreibungs- und Konkursrechts kann sich erledigen. Jedes weitere öffentlich zugänglich machen dieser Daten ist damit aus datenschutzrechtlicher Sicht grundsätzlich nicht zulässig, es sei denn, es wird an derselben Stelle auch über die Erledigung der Sache informiert. Dies ist jedoch illusorisch: Die Information über die Tilgung einer Schuld wird nirgendwo öffentlich und damit auch nicht im Internet festgehalten, so dass das Bild des säumigen Schuldners bestehen bleibt. Auch eine verurteilte Person wird mit der Publikation des Urteils im Internet den «Makel» der einmal gegen sie eröffneten Strafverfolgung nicht nur nicht beheben können, sie kann auch keine Beweise zur Art der Vollstreckung der Strafe oder allfälligen Strafvollzugsmilderungen wegen guter Führung anbringen: Im Internet bleibt nur das Strafurteil zugänglich. Weltweit. Jederzeit.

[Rz 32] Die Möglichkeit, an einem anderen Ort «von neuem anzufangen», oder eine erfolgreiche Resozialisierung zu erfahren, bleibt damit unweigerlich verwehrt, was nach der Auffassung der Autorin eine ausgesprochen problematische Entwicklung darstellt.

1.3. Regelungsbedarf und -möglichkeiten

[Rz 33] Sowohl die Rechtsprechung des EuGH wie auch die Bemühungen der Europäischen Union haben die Problematik, dass das Internet nie vergisst, aufgenommen[36]: Mit dem «Recht auf Vergessen» soll eben dieser Neustart, die Resozialisierung ermöglicht werden. Ob dieses Recht auf Vergessen aber nicht ein blosses Lippenbekenntnis bleibt, ja in Anbetracht der de facto Unmöglichkeit der Löschung von Internet-Einträgen bleiben *muss*, ist derzeit umstritten[37]. Und was bereits für den privatrechtlichen Bereich problematisch erscheint, wird in öffentlich-rechtlichen Belangen umso komplexer: Hat der Staat nicht gar eine gewisse Verantwortung, ursprünglich öffentliche Informationen nach einer gewissen Zeit zumindest nicht mehr ganz so einfach zugänglich zu machen? Darf der Staat in Anbetracht des Internet-Grundsatzes «einmal öffentlich, immer öffentlich»

36 Wenn auch «nur» im privatrechtlichen Bereich, so in der EU-Datenschutzgrundverordnung (siehe dazu die Zusammenfassung des Verhandlungsführers des Europäischen Parlaments Jan Philipp Albrecht auf https://www.janalbrecht.eu/fileadmin/material/Dokumente/Datenschutzreform_Stand_der_Dinge_10_Punkte_110615.pdf) und im Entscheid EuGH, Rs. C-131/12, ECLI:EU:C:2014:317 (Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González).

37 Vgl. dazu zum in Fn 37 genannten Urteil die kritischen Schlussanträge des Generalanwalts Niilo Jääskinen vom 25. Juni 2013, ECLI:EU:C:2013:424 sowie die Kritik von Daniel Hürlimann, Das Google-Urteil des EuGH und die Entfernungspflicht von Suchmaschinen nach schweizerischem Recht, sui-generis, 30. August 2014, abrufbar unter http://sui-generis.ch/1#note-34.

überhaupt Personendaten online zugänglich machen, im vollen Bewusstsein, dass es sich dabei um Daten mit besonderem Stigmatisierungsrisiko handelt?

[Rz 34] Die aktuellen gesetzlichen Grundlagen zur Veröffentlichung von beispielsweise Betreibungsurkunden oder Strafurteilen gehen auf diese Problematik nicht ein: Art. 35 Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) sieht schlicht vor: «Die öffentlichen Bekanntmachungen erfolgen im Schweizerischen Handelsamtsblatt und im betreffenden kantonalen Amtsblatt.» Ähnlich kurz angebunden ist auch Art. 88 Strafprozessordnung (StPO):

> «[1] *Die Zustellung erfolgt durch Veröffentlichung in dem durch den Bund oder den Kanton bezeichneten Amtsblatt, wenn: a. der Aufenthaltsort der Adressatin oder des Adressaten unbekannt ist und trotz zumutbarer Nachforschungen nicht ermittelt werden kann; b. eine Zustellung unmöglich ist oder mit ausserordentlichen Umtrieben verbunden wäre; c. eine Partei oder ihr Rechtsbeistand mit Wohnsitz, gewöhnlichem Aufenthaltsort oder Sitz im Ausland kein Zustellungsdomizil in der Schweiz bezeichnet hat. (…)* [3] *Von Endentscheiden wird nur das Dispositiv veröffentlicht.*»

[Rz 35] Dass weder SchKG noch StPO über den Inhalt der Veröffentlichung hinausgehende Vorgaben wie beispielsweise zur *Form* oder zur *Dauer* der Publikation machen, findet seine Ursache im föderalistischen Prinzip, wonach die Kantone für die konkrete Umsetzung des Schuldbetreibungs- und Konkurs- oder Strafprozessrechts[38] (bzw. für die Organisation ihrer amtlichen Publikationen) zuständig sind. Die diesbezüglich getroffenen Lösungen sind typisch-schweizerisch vielfältig:

- Der Kanton Basel-Stadt verfügt derzeit noch[39] über keine Bestimmungen, die eine Online-Publikation des Amtsblatts vorsehen würden, gleiches gilt beispielsweise für die Kantone Graubünden, Jura oder Uri – obschon das Amtsblatt dieser drei Kantone online und ohne Restriktionen, wie beispielsweise der Pflicht zur Eröffnung eines Benutzerkontos, abgerufen werden kann.
- Hingegen verfügt der Kanton Basel-Landschaft zwar nicht über eine formell-gesetzliche Grundlage für die Online-Publikation des Amtsblattes (sondern nur über eine formell-gesetzliche Grundlage für die Papier-Version), hält aber in seiner Verordnung über das Internet-Amtsblatt[40] fest, welche Informationen für wie lange im Internet zugänglich gemacht werden sollen. So sieht § 1 Abs. 2 lit. d der besagten Verordnung beispielsweise eine Verweildauer von 6 Monaten für Publikationen der Betreibungs- und Konkursämter vor. Die Veröffentlichung von Urteilsdispositiven im Internet-Amtsblatt scheint nicht vorgesehen zu sein.
- Der Kanton Zug wiederum, um einen anderen Lösungsansatz zu nennen, sieht im Publikationsgesetz[41] sowohl die Papier- wie auch die Online-Publikation des Amtsblattes vor, und delegiert dabei die Festlegung der Fristen für die Zugänglichkeit an den Regierungsrat.
- Als dritte Variante sehen die Kantone Fribourg[42] und Tessin[43] zwar ebenfalls eine Papier- und eine Online-Publikation vor, legen dabei aber keinerlei Fristen für die Veröffentlichung im

38 Art. 122 bzw. Art. 123 der Schweizerischen Bundesverfassung vom 18. April 1999 (BV, SR 101).

39 Ein Entwurf für ein Publikationsgesetz befand sich zum Zeitpunkt der Abgabe dieses Artikels in der kantonsinternen Vernehmlassung.

40 Basellandschaftliche Verordnung vom 26. Juni 2007 über das Internet-Amtsblatt (SGS 106.12).

41 § 6 Abs. 3 des Zuger Gesetzes vom 29. Januar 1981über die Veröffentlichung der Gesetze und das Amtsblatt (BGS 152.3).

42 Art. 1 der Freiburger Verordnung vom 21. Dezember 2010 über das Amtsblatt (RFS 124.21).

43 Art. 4 des Tessiner regolamento del 15 aprile 2015 sulle pubblicazioni ufficiali (RL 1.7.3.1.1).

Internet fest.

- Der Kanton Glarus, um die letzte Variante aufzuzeigen, sieht Folgendes vor: «Das Amtsblatt wird im Internet veröffentlicht; der Zugang ist unentgeltlich. Es erscheint zudem in gedruckter Form und kann in der Staatskanzlei eingesehen werden.»[44]

[Rz 36] Damit wird augenscheinlich, dass mit der Problematik der weltweiten Öffentlichkeit des Internets nicht nur ganz unterschiedlich umgegangen wird, sondern dass zumindest in einzelnen Kantonen durchaus auch ein Bewusstsein dafür besteht, dass Personen, die einmal im Amtsblatt erwähnt wurden, nach einer gewissen Zeit auch die Möglichkeit gegeben werden muss, ohne den Rucksack der öffentlichen Stigmatisierung aufgrund einer veröffentlichten Betreibungsurkunde oder eines veröffentlichten Strafurteilsdispositivs durch das weitere Leben zu gehen.

[Rz 37] Dass das Bewusstsein für diesen Anspruch besteht, ist grundsätzlich erfreulich. Realistischerweise muss sich das für die Veröffentlichung des Amtsblattes im Internet verantwortliche Organ aber auch eingestehen, dass auch eine nur vorübergehende Publikation de facto dazu führen kann, dass der besagte Eintrag noch Jahre nach der Löschung abgerufen werden kann, wenn Seiten gespiegelt, Informationen übertragen oder PDF-Files in andere Webseiten übernommen wurden. Dies soll jedoch nicht bedeuten, dass auf die Festlegung einer Veröffentlichungsdauer verzichtet werden kann, oder dass – das andere Extrem – gänzlich auf die Online-Publikation des Amtsblattes verzichtet werden muss. Letzteres wäre schlicht nicht mehr zeitgemäss, ersteres würde von mangelndem Verantwortungsbewusstsein zeugen. Die im vollen Bewusstsein der Internet-Problematik erfolgende Festlegung einer spezifischen Verweildauer von Amtsblatt-Publikationen, die Personendaten enthalten, ist aus datenschutzrechtlicher Sicht durchaus angezeigt: Zum einen, um das Prinzip der Verhältnismässigkeit (wenigstens im Ansatz und aus Sicht der öffentlichen Verwaltung) zu wahren und zum anderen, um immerhin gewisse Hürden für die Wiederauffindung einzelner ehemals im Amtsblatt erwähnter Personen zu setzen.

[Rz 38] Nicht minder problematisch als der aus Resignation über die Unzulänglichkeiten des Internets erfolgte Verzicht auf die Festlegung von Veröffentlichungszeiträumen wäre es aber auch, wenn diejenigen Kantone, die bislang über keine Bestimmungen zur Internet-Publikation des Amtsblattes verfügen, weiterhin auf die althergebrachten Bestimmungen zur Print-Version bauen würden, gleichzeitig aber das Amtsblatt ohne Einschränkungen im Internet zugänglich machen. Der derzeit vom Kanton Basel-Stadt verfolgte Weg, wonach Abonnentinnen und Abonnenten des Kantonsblattes einen Zugang zum Online-Archiv erhalten, allen anderen interessierten Personen jedoch nur die Papier-Version des Kantonsblattes (und damit letztendlich der Gang ins Archiv, wenn ältere Informationen gesucht werden), offen steht, erscheint diesbezüglich als gelungen.

[Rz 39] Damit wird deutlich: Eine aus rechtstaatlicher Sicht perfekte Lösung kann nicht gefunden werden, wenn amtliche Informationen im Internet veröffentlicht werden sollen. Umso wichtiger ist es daher, dass klare Vorgaben gemacht und Anstrengungen unternommen werden, damit der staatlichen Verantwortlichkeit bei der Publikation von Personendaten im Amtsblatt nachgekommen und das Risiko von Persönlichkeitsverletzungen zumindest von staatlicher Seite so weit als möglich minimiert werden kann.

---

44 Art. 8 des Glarner Publikationsgesetzes vom 4. Mai 2014 (GSI D/24/1).

2. Das digitale Archiv

[Rz 40] Auch die *Archivierung* von Personendaten stellt ein Datenbearbeiten dar und muss sich daher nach den Vorgaben des jeweiligen (Informations- und) Datenschutzgesetzes richten: Die entsprechenden gesetzlichen Grundlagen finden sich, wie vorangehend bereits angesprochen, in den Archivgesetzen – die allgemeinen Datenschutzgrundsätze gelten weiterhin auch für diese Form der Datenbearbeitung.

[Rz 41] Ein Blick in die Archivgesetze und die dazugehörigen Verordnungen zeigt: Derzeit wird von primär papierbasierten Archiven ausgegangen, welche vor Ort eingesehen werden können. Selbstverständlich verfügen die Archive über digitale Kataloge, welche die Recherche nach den gewünschten Dokumenten vereinfachen. In der Regel ist es aber noch nicht möglich, die jeweiligen Dokumente direkt am heimischen PC einzusehen. Dies soll sich aber in naher Zukunft ändern. So verfolgen beispielsweise die Kantone Basel-Stadt und St. Gallen derzeit das Projekt «digitalAccess2Archives»[45]: In den vergangenen Jahren lag der Fokus der Archive primär im Bereich der Digitalisierung der Archivalien – d.h. in der Digitalisierung ursprünglich analogen Archivgutes, der Zurverfügungstellung digitaler Daten bzw. der Sicherung dieser Daten für die weitere Zukunft sowie der Erstellung von Konzepten für die Verwaltung und Erstellung digitaler Akten bereits im Verwaltungsalltag. «DigitalAccess2Archives» dreht sich nun um den *Zugang* zu den digitalen Archivalien, kurz, um den digitalen Lesesaal. Und damit nicht genug: Auch die sich langsam entwickelnden eGovernment-Services, Open Government Data und Big Data sollen in diesem Projekt ebenso berücksichtigt werden wie Social Media Services[46].

[Rz 42] Das Bild des Archivs wird sich damit fundamental ändern. Die damit verbundenen Herausforderungen sind immens, und reichen – aus datenschutzrechtlicher Sicht – vom Benutzermanagement bis hin zu «klassischen» Informationssicherheitsfragen:

2.1. Herausforderungen

a) Schutz vor unberechtigten Zugriffen

[Rz 43] Vor dem Zeitalter der digitalen Lesesäle bzw. der «papierlosen Verwaltung» und damit verbunden der papierlosen Archive konnten Archivarinnen und Archivare vor dem Zugriff einer Person auf die Archivalien prüfen (oder zumindest plausibilisieren), ob der Zugang zu den gewünschten Daten berechtigterweise erfolgt. Forscher hatten ihre Forschungsprojekte zu umreissen, betroffene Personen hatten ihre Identität nachzuweisen. Die Herausforderung, die sich diesbezüglich mit der Digitalisierung der Archive stellt, ist immens: Welche Berechtigungen sind wie zu vergeben? Wie kann verifiziert werden, dass die Person, die bestimmte Daten aus dem Archiv abrufen will, auch tatsächlich dazu berechtigt ist? Vor unberechtigten Zugriffen auf Archivdaten sind dabei nicht nur diejenigen Personen zu schützen, deren Daten im Archiv vorhanden sind. Vielmehr können auch Nutzerinnen und Nutzer der Archive Opfer von Persönlichkeitsverletzungen sein, wenn von Unberechtigten beispielsweise Profile, Suchverläufe und Bestelllisten eingesehen werden können. Je nach politischer und gesellschaftlicher Situation könnten gewisse Recherchethemen plötzlich zu

45 http://www.staatsarchiv.sg.ch/home/auds/18/__jcr_content/Par/downloadlist_3/DownloadListPar/download_0.ocFile/Praesentation%20Kansy%20Luethi.pdf.

46 Machbarkeitsstudie «Projekt Digital Access 2 Archives», dem Datenschutzbeauftragten des Kantons Basel-Stadt im Rahmen der Projektberatung vorgelegt.

Repressionen führen. Es ist aber durchaus auch denkbar, dass konkurrierende Forschungsteams auf unlautere Methoden zurückgreifen, um herauszufinden, welche Anfragen andere Forscherinnen und Forscher getätigt haben etc.

[Rz 44] Entsprechend hohe Anforderungen müssen an die Schutzvorkehrungen gestellt werden, welche unberechtigte Zugriffe auf die Archivalien und auf die Nutzerdaten verhindern sollen. Die aktuellen Archivgesetze und die entsprechenden Nutzerreglemente mögen zwar Vorgaben zum Zugang zu den Archivalien sowie allgemeine Sicherungspflichten des Archivs enthalten – mit der Digitalisierung der Archive müssen diese Vorgaben aber zwingend überarbeitet werden. Andernfalls nach der hier vertretenen Auffassung erhebliche Defizite bei den für die Archivbewirtschaftung erforderlichen gesetzlichen Grundlagen entstehen. Ob bereits auf Gesetzesstufe bestimmte allgemeine Vorgaben gemacht werden können, oder ob es allenfalls nicht praktikabler wäre, in einfach anpassbaren Nutzerreglementen Vorgaben zur machen, ist zu diskutieren und je nach konkretem System zu entscheiden.

b) Unbefugte Veränderung

[Rz 45] Die Integrität von archivierten Dokumenten zu wahren, stellte bislang keine grosse Herausforderung dar: Papierakten konnten vor Ort im Original eingesehen werden, ein Verändern, ohne dass dies nicht sofort sichtbar gewesen wäre, war jedoch bislang nicht möglich. Und auch die Veränderung von beispielsweise mittels Scans nachträglich digitalisierten Akten wird, je nach Dateiformat, auch weiterhin nur schwer möglich sein. Sobald sich aber die «papierlose Verwaltung» etabliert hat und die jeweiligen Akten entsprechend auch originär-digital archiviert werden, besteht das Risiko, dass die Dokumente bei ungenügender Sicherung manipuliert werden können.

[Rz 46] Es wird in diesem Zusammenhang unumgänglich sein, dass sich die Archive über die neusten Schutzwerkzeuge auf dem Laufenden halten – denn auch ein ursprünglich vor Veränderungen geschütztes Dokument kann unter Umständen dank dem technischen Fortschritt in ein paar Jahren ohne weiteres verändert werden. Gleichzeitig stellt sich aber auch die Frage, ob eine Bestimmung im Sinne von «das Staatsarchiv sichert die dauerhafte Erhaltung sowie Benützbarkeit des Archivgutes und schützt es vor unbefugter Benützung oder Vernichtung»[47] hier noch zu genügen vermag, oder ob nicht zumindest auf ein Sicherheitskonzept, welches als Verordnung oder als Anhang zum Gesetz erlassen werden kann, verwiesen werden müsste.

c) Unbefugte Löschung/Vernichtung von Daten

[Rz 47] So banal es sich auch anhören mag: Die Archive müssen darum besorgt sein, dass archivierte digitale Akten nicht unbefugter Weise vernichtet werden. Das Risiko, dass Papierdossiers von Nutzerinnen oder Nutzern vernichtet werden, dürfte vergleichsweise klein sein, da die Dokumente die Archivräumlichkeiten üblicherweise nicht verlassen und nur unter Aufsicht eingesehen werden dürfen. Werden jedoch digitale Archivalien zur Verfügung gestellt, so muss zwingend mittels entsprechender Sicherheitsvorkehrungen (Schutz der Server, Schreib-/Löschschutz der Dokumente,

[47] So beispielsweise die Formulierung in § 6 des baselstädtischen Gesetzes vom 11. September 1996 über das Archivwesen (SG 153.600), ähnlich aber auch die Wortwahl des § 13 des Zürcher Archivgesetzes vom 24. September 1995 (LS 170.6): «Die Archive unterhalten die Akten sorgfältig, fachgerecht und reproduzierbar, sie sichern sie gegen Verderb und Verlust und führen über sie ausführliche Verzeichnisse.»

genaues Login der Nutzerbewegungen etc.) dafür gesorgt werden, dass keine findigen vermeintlichen Archivnutzerinnen oder -nutzer die Dossiers – sei dies aus Jux, sei dies, um gewisse Ereignisse vergessen zu machen – löschen können. Ähnlich wie im Falle der unbefugten Veränderung enthalten die Archivgesetze derzeit zwar die Pflicht der Archivare, das Archivgut vor unbefugter Vernichtung zu schützen – mit den digitalen Archiven wird dieser Auftrag jedoch eine neue Dimension erhalten.

2.2. Handlungsbedarf

[Rz 48] Allein diese drei Themenkomplexe zeigen, dass der Handlungs- bzw. Diskussionsbedarf mit zunehmender Digitalisierung der Archive wächst und dringlicher wird. Diskussionsbedarf besteht dabei jedoch nicht nur zwischen Archivverantwortlichen und Informatikspezialistinnen und -spezialisten, wobei es gilt, eine gemeinsame Sprache zu finden, Risikoanalysen zu erstellen und basierend auf diesen Einschätzungen Lösungen zu entwickeln, die die archivierten Daten angemessen schützen und gleichzeitig die Balance zwischen den Interessen der Archive, der Betroffenen und der Nutzerinnen oder Nutzer zu wahren. Es muss auch eine rechtliche Beurteilung der digitalen Archive erfolgen, denn es erschiene kurzsichtig, die bestehenden Archivgesetze angesichts der neuen Möglichkeiten und Risiken nicht zu aktualisieren und in ihrer von einer analogen Gesellschaft und Verwaltung ausgehenden Konzeption zu belassen.

3. Digitale Nummernschilderfassung

3.1. Technische Möglichkeiten

[Rz 49] Die Erfassung von Nummernschildern ist keine neue Entwicklung: Während bei den seit 1950er Jahren[48] vorgenommenen Geschwindigkeitsmessungen mit statischen Radargeräten («Blitzer») die Nummernschilder der Verkehrssünderinnen und -sünder fotografiert und dann von Mitarbeiterinnen und Mitarbeitern im Büro mit den jeweiligen Datenbanken abgeglichen werden, werden die Nummernschilder bei den sogenannten Abschnittsgeschwindigkeitskontrollen von einem Scanner zu Beginn und am Ende eines bestimmten Streckenabschnitts eingelesen, bei vorschriftsgemässer Geschwindigkeit innerhalb des jeweiligen Abschnitts automatisch wieder gelöscht oder bei zu hohem Tempo gespeichert und zur Auswertung an die zuständige Polizeibehörde übermittelt.

[Rz 50] Ebenso werden im Ausland seit längerem[49] sogenannte statische «CatchKen» Bildanalysesysteme insbesondere bei der Fahndung nach gesuchten Fahrzeugen, der Ermittlung gestohlener Fahrzeuge oder der Ermittlung von nicht versicherten Fahrzeugen eingesetzt. Wesentliches Merkmal dieser statischen «CatchKen»-Systeme ist, dass sie an einem bestimmten Ort für einen gewissen Zeitraum fix installiert werden – also beispielsweise entlang einer Hauptstrasse, welche an eine Landesgrenze führt – und dass die Nummern vor Ort direkt mit einer auf einem Laptop hinterlegten Datenbank bzw. einem Datenbankauszug offline abgeglichen werden. Wird ein nicht versichertes oder gestohlenes Fahrzeug identifiziert, so besteht für die diensthabenden Polizistinnen und Polizisten die Möglichkeit, die Verfolgung aufzunehmen.

[Rz 51] Der technische Fortschritt erlaubt es nun, «CatchKen» mobil einzusetzen und die jeweiligen

48 https://de.wikipedia.org/wiki/Geschwindigkeits%C3%BCberwachung.

49 Erster Einsatz Mitte der 90er Jahre des letzten Jahrhunderts, siehe dazu http://www.vidit-systems.de/index.php/kennzeichenerkennungssysteme/catch-ken-mobile-und-stationaere-kennzeichenerkennungssysteme.

Datenbanken sogar online abzurufen. Die in den Polizeifahrzeugen installierten Systeme lassen sich entweder bei einem konkreten Verdacht einschalten oder aber vollautomatisch, mit dem Drehen des Zündschlüssels, in Betrieb nehmen[50].

3.2. Fragestellungen

a) Genügende gesetzliche Grundlage?

[Rz 52] Es gehört zweifelsohne zu den polizeilichen Aufgaben, säumige Fahrzeugsteuerzahlerinnen und -zahler aufzuspüren und nach gestohlenen Fahrzeugen und flüchtigen Personen zu fahnden. Gestützt auf Art. 5 i.V.m. Art. 36 BV müssen diese Aufgaben aber in einer genügend bestimmten gesetzlichen Grundlage festgehalten sein[51]. So weist denn auch die Verordnung des Bundes vom 28. März 2007 über die Kontrolle des Strassenverkehrs[52] die Zuständigkeit für die Kontrollen des öffentlichen Verkehrs den kantonalen Polizeibehörden zu, wobei die kantonalen Polizeibehörden den jeweiligen modus operandi festzulegen haben. Ein Blick in die kantonalen Polizeigesetze und -verordnungen bringt diesbezüglich aber Ernüchterung: So findet sich im Kanton Basel-Stadt wohl eine allgemeine Umschreibung der polizeilichen Aufgaben im Polizeigesetz, aber nirgendwo eine konkrete Bestimmung zur Verkehrsüberwachung oder Fahrzeugfahndung. Gleiches gilt, um nur ein paar zu nennen, beispielsweise auch für die Kantone Bern, Zürich und Graubünden, sowie für die Kantone Fribourg und Tessin.

[Rz 53] Mit viel gutem juristischen Willen und unter Berücksichtigung der eher geringen Schwere des Eingriffs in die Persönlichkeitsrechte der betroffenen Personen kann der nicht-automatisierte Abgleich von Listen säumiger Fahrzeugsteuerzahlerinnen und -zahler wohl unter die SKV-Bestimmungen sowie die allgemeinen Aufgabenumschreibungen in den kantonalen Polizeigesetzen subsumiert und die gesetzliche Grundlage damit als gegeben betrachtet werden: Zum einen kann bei einem von Menschen vorgenommenen Abgleich keinesfalls von einer flächendeckenden Kontrolle ausgegangen werden. Vielmehr handelt es sich bei dieser Form der «Fahndung» um Stichprobenkontrollen oder mehr oder weniger gezieltes Suchen, womit die übrigen geparkten Fahrzeuge bzw. deren Halterinnen und Halter nicht unter einen Generalverdacht fallen, nicht automatisch mit der jeweiligen Datenbank abgeglichen und damit auch nicht (je nach Einstellung des Systems auch nur für Sekundenbruchteile) in einem Informatiksystem gespeichert werden (sondern wohl in begrenztem Rahmen im Gedächtnis der Polizistin oder des Polizisten).

[Rz 54] Sobald aber flächendeckend automatisierte Abgleiche vorgenommen werden sollen, dürften angesichts der damit verbundenen deutlich grösseren Schwere des Grundrechtseingriffs die aktuell bestehenden gesetzlichen Grundlagen nicht mehr ausreichend sein, auch wenn die SKV den Einsatz technischer Hilfsmittel grundsätzlich erlaubt. So hat denn auch der Kanton Basel-Landschaft per 15. Juni 2014 eine Bestimmung in Kraft gesetzt, welche die automatische Fahrzeugfahndung und Verkehrsüberwachung regelt:

> «[1] *Die Polizei Basel-Landschaft kann Kontrollschilder von Fahrzeugen automatisiert*

---

50 http://www.vidit-systems.de/index.php/kennzeichenerkennungssysteme/catch-ken-on-kennzeichenerfassung-aus-dem-fahrenden-fahrzeug; http://www.bredar.ch/index.php/de/catch-ken.

51 Rechtssätze müssen folglich ein voraussehbares, berechenbares und rechtsgleiches Verwaltungshandeln sicherstellen und daher ein hinreichen- des und angemessenes Mass an Bestimmtheit aufweisen (statt vieler BGE 130 I 1, E. 3.1).

52 Strassenverkehrskontrollverordnung, SKV, SR 741.013.

> *erfassen und mit Datenbanken abgleichen.* [2] *Der automatisierte Abgleich ist zulässig: a. mit polizeilichen Personen- und Sachfahndungsregistern; b. mit durch die Polizei Basel-Landschaft erstellten Listen von Kontrollschildern von Fahrzeugen, deren Halterinnen oder Halter der Führerausweis entzogen oder verweigert worden ist; c. mit konkreten Fahndungsaufträgen der Polizei Basel-Landschaft.* [3] *Die automatisch erfassten Daten werden wie folgt gelöscht: a. sofort in den Fällen ohne Übereinstimmung mit einer Datenbank; b. im Falle einer Übereinstimmung mit einer Datenbank gemäss den Bestimmungen des betreffenden Verwaltungs- oder Strafverfahrens.*»[53]

[Rz 55] Dieser Ansatz ist grundsätzlich zu begrüssen und sollte von denjenigen Kantonen, die einen Einsatz automatischer Nummernschilderkennungssysteme in Erwägung ziehen, als Vorbild in die Projektarbeiten miteinbezogen werden: Die Bestimmung umschreibt klar, was die Kantonspolizei tun darf, welche Datenbanken dazu genutzt werden dürfen und wann die Daten gelöscht werden müssen. Wünschenswert wäre jedoch zumindest ein Hinweis auf ein auszuarbeitendes Informationssicherheitskonzept gewesen (dazu sogleich lit. b).

b) Informationssicherheit

[Rz 56] Wie bereits mehrfach angesprochen, ergeben sich mit dem Wechsel von «Manpower» auf technische Hilfsmittel diverse informationssicherheitsrechtliche Herausforderungen, die natürlich auch im Falle von mobilen Nummernschilderkennungssystemen berücksichtigt und überwunden werden müssen:

[Rz 57] Wenn die automatische Nummernschilderkennung so konfiguriert ist, dass sie bereits mit dem Starten des Motors des Polizeifahrzeugs in Betrieb genommen wird, stellt sich die Frage, wie sichergestellt werden kann, dass tatsächlich nur jene Polizistinnen und Polizisten das mit «CatchKen» ausgestattete Fahrzeug nutzen, die dies zu ihrer Aufgabenerfüllung tun dürfen. Aus Kostengründen werden wohl ohnehin nicht sämtliche Polizeifahrzeuge mit einer derart konfigurierten automatischen Nummernschilderkennung ausgestattet werden – gleichwohl muss mittels interner Reglemente und klarer Dienstanweisungen sichergestellt werden, dass die automatische Nummernschilderkennung tatsächlich nur zur Aufgabenerfüllung und nicht «beiläufig» von anderen als den zuständigen Polizistinnen und Polizisten im Rahmen derer Aufgabenerfüllung eingesetzt wird: So erschiene es beispielsweise problematisch, wenn eine Mitarbeiterin des Sozialdienstes der Polizei ein mit CatchKen ausgestattetes Fahrzeug nutzt, um zu einem Beratungsgespräch mit einem Opfer häuslicher Gewalt zu fahren, und unterwegs säumige Fahrzeugsteuerzahlerinnen und -zahler registrieren würde.

[Rz 58] Muss die Nummernschilderkennung erst aktiv in Betrieb genommen werden, so ist sicherzustellen, dass dies wiederum nicht von «jedermann» getan werden kann. Idealerweise wird die Inbetriebnahme nur mittels Eingabe eines persönlichen Passworts (und nicht etwa eines Dienstgruppen-Passworts!) ermöglicht, so dass nachvollzogen werden kann, wer zu welchem Zeitpunkt mit dem Fahrzeug unterwegs war. Entsprechend sind auch Log-Files zu erstellen, wobei darauf zu achten ist, dass in den Logs tatsächlich nur die erforderlichen Daten zur Kontrolle der Mitarbeiterinnen und Mitarbeiter, nicht aber beispielsweise die abgeglichenen Autonummern verzeichnet werden – letzteres würde einer unzulässigen Aufbewahrung der nicht weiter erforderlichen Daten derjenigen

53 Basellandschaftliches Polizeigesetz vom 28. November 1996, SGS 700.

Fahrzeughalterinnen und -halter, die ihre Steuern bezahlt haben etc., gleichkommen.

[Rz 59] Stichwort Speicherung – dieses Thema ist ganz grundsätzlich sorgfältig zu erarbeiten, denn mit der elektronischen Erfassung der geparkten Fahrzeuge werden deren Nummernschilder zumindest solange, wie der Abgleich mit der jeweiligen Datenbank erfolgt, in einem Arbeitsspeicher aufbewahrt. Dies kann grundsätzlich als notwendig erachtet werden, sobald aber ein negatives Ergebnis der Prüfung vorliegt, müssen die Autonummern unwiederbringbar gelöscht werden. Andernfalls würde, ähnlich der soeben illustrierten Speicherung der Nummern in Logfiles, eine unzulässige Speicherung vorliegen, welche den Vorgaben des Verhältnismässigkeitsgrundsatzes nicht gerecht wird.

[Rz 60] Natürlich ist auch dem Risiko, dass nicht mehr aktuelle Daten genutzt werden, Rechnung zu tragen: Wie wird sichergestellt, dass die eingelesenen Nummernschilder mit den aktuellen Datensätzen abgeglichen werden? Was bei Online-Abgleichen kein Problem ist, erfordert bei offline-Zugriffen auf im Fahrzeug oder auf USB-Sticks gespeicherte Listen klare Update-Abläufe. Kann sichergestellt werden, dass z.B. die Fahrzeugdatenbank automatisch aktualisiert wird, bestehen klare Verantwortlichkeiten zur Aktualisierung der externen Speichermedien?

[Rz 61] Und zu guter Letzt ist dafür zu sorgen, dass bei Online-Lösungen, also bei Geräten, die die jeweiligen abzufragenden Datenbanken nicht lokal im Fahrzeug, sondern auf externen Servern nutzen, keine unberechtigten Zugriffe erfolgen können, dass die Systeme also mittels Firewalls etc. so geschützt werden, dass Hacker keinen Zugang zu den Datenbanken via Fahrzeug erlangen können.

3.3. Handlungsbedarf

[Rz 62] Bereits heute gründet der Abgleich von Nummernschildern mit Listen säumiger Fahrzeugsteuerzahlerinnen und -zahler auf eher dünnen bzw. «zusammengeflickten» gesetzlichen Grundlagen, welche den betroffenen Personen ein ausgesprochen geringes Mass an Rechtssicherheit zu vermitteln mögen. Der Einsatz digitaler Nummernschilderkennungssysteme wird von den Polizeibehörden bzw. vom Gesetzgeber daher weitreichende Regelungsarbeiten erfordern: Zum einen muss der automatische Nummernschildabgleich nach der hier vertretenen Auffassung zwingend in einem Gesetz im formellen Sinne explizit geregelt werden, da der mit dem automatischen Abgleich einhergehende Grundrechtseingriff als deutlich schwerer zu beurteilen ist als im Falle der bisherigen Abgleiche «von Auge» durch die Polizistinnen und Polizisten beim Gang durch's Quartier. Gleichzeitig bietet die Regelung im Gesetz die Möglichkeit, gewisse Rahmenbedingungen wie beispielsweise die Aufbewahrungsdauer der gescannten Nummernschilder oder die Update-Modalitäten festzulegen. Und schliesslich kann im Gesetz auch der Auftrag zur Ausarbeitung des zwingend erforderlichen Informationssicherheitskonzepts erteilt werden. Dieses Informationssicherheitskonzept muss von den verantwortlichen Stellen innerhalb der jeweiligen Kantonspolizei gemeinsam mit den kantonalen Informationssicherheits-Spezialisten und der oder dem Datenschutzbeauftragten erarbeitet werden.

[Rz 63] Mit dem Beispiel des automatisierten Nummernschildabgleichs lässt sich eindrücklich illustrieren, wie mit einer verhältnismässig unscheinbaren Erleichterung des Arbeitsalltags – dem Wandel von von Menschen-Auge durchgeführten Abgleichen zu digitalen Abgleichen – deutlich schwerwiegendere Eingriffe in die Persönlichkeitsrechte der betroffenen Personen einhergehen können. Das Argument «Das haben wir schon immer so gemacht, nun machen wir es einfach mit anderen Hilfsmitteln», dürfte damit endgültig entkräftet sein.

IV. Lösungsansätze

1. Rechtlicher Handlungsbedarf?

[Rz 64] Der Einsatz neuer Technologien lässt meistens auch den Ruf nach neuen Regelungen laut werden. Auch bezüglich der vorangehend erläuterten Beispiele hat sich gezeigt, dass durchaus rechtlicher Regelungsbedarf besteht, dass sich dieser jedoch je nach Themenkreis gänzlich unterschiedlich gestaltet: Je nach Intensität der mit dem Einsatz der neuen Technologien verbundenen Eingriffe in die Persönlichkeitsrechte der Betroffenen, je nach Menge der Daten, je nach Ausgestaltung der neuen technischen Möglichkeiten, können die neuen Technologien unter die bestehenden Rechtsgrundlagen für die jeweilige Aufgabenerfüllung subsumiert werden, bedarf es allenfalls einzelner Anpassungen oder gar gänzlich neuer Bestimmungen und Konzeptionen: So sollte beispielsweise ganz grundsätzlich thematisiert werden, ob die bestehenden Bestimmungen zur Veröffentlichung von Informationen über Personen in der StPO, dem SchKG oder den anderen Gesetzen die Veröffentlichung im Internet ebenfalls vorhergesehen haben – bei der vergleichsweise neuen StPO dürfte dies sicherlich der Fall sein, beim über 100 Jahre alten SchKG zweifelsohne nicht. Besteht hier Handlungsbedarf? Muss das Konzept der Zustellungsfiktion in Anbetracht der internet-bedingten «unumkehrbaren Weltöffentlichkeit» von Grund auf überdacht werden? Diese Fragen müssen hier vorerst offen bleiben – sie dürfen jedoch nicht in Vergessenheit geraten.

[Rz 65] Gleichwohl ist die Schaffung neuer formell-gesetzlicher Regelungen nach der hier vertretenen Auffassung nicht die Lösung aller Probleme, und führt keineswegs zur Behebung sämtlicher Risiken. In Anbetracht der relativen Trägheit der Rechtssetzungsprozesse wird es nur schwer realisierbar sein, dass die jeweiligen gesetzlichen Grundlagen den aktuell genutzten technischen Möglichkeiten tatsächlich entsprechen bzw. diesen einen Rahmen setzen. Entsprechend bedacht sollte die Anpassung der rechtlichen Grundlagen daher vorgenommen werden: Es kann gar genügen, dass – wie beispielswiese im Falle der digitalen Amtsblätter – die Digitalisierung der Arbeitsvorgänge aufgenommen oder einzelne genutzte Systeme – wie im Falle der von den Kantonspolizeien genutzten Informationssysteme – explizit erwähnt werden, dass darüber hinaus aber lediglich eine (klar umschriebene!) Delegation weiterer Regelungsthemen stattfindet, so beispielsweise bezüglich der Löschfristen, der Informationssicherheitsvorgaben oder der Regelung der Verantwortlichkeiten. Derartige Regelungen können ohne grossen Aufwand regelmässig auf ihre Aktualität hin überprüft und bei Bedarf relativ unbürokratisch angepasst werden.

[Rz 66] Diese Relativierung des Rufs nach rechtlichen Regelungen soll jedoch nicht dazu führen, dass der Auffassung «Wir machen ja das gleiche wie bis anhin, einfach mit anderen Mitteln» gefolgt und auf die kritische Prüfung der bestehenden Rechtsgrundlagen verzichtet wird. Vielmehr ist die Schaffung von übereilten und wenig aussagekräftigen rechtlichen Scheinlösungen zu vermeiden: Der Einsatz neuer Technologien erfordert ein solides rechtliches Fundament, bedingt aber auch weitreichende organisatorische Regelungen und Konzepte, wie im Folgenden illustriert werden soll.

2. Neue Technologien, neue Ansätze: IT-Governance und gelebte Verantwortung

[Rz 67] Aktualisierte formell-gesetzliche Grundlagen können dem Verwaltungsalltag lediglich Leitplanken vorgeben, innerhalb derer die jeweiligen Aufgaben zu erfüllen und die neuen technischen Hilfsmittel zu nutzen sind. Es braucht jedoch weitaus mehr, denn eine gesamtkantonale Strategie zur Nutzung von IT-Mitteln und ohne dienststellenbezogene detailliertere Vorgaben (beispielsweise

in Verordnungen, internen Richtlinien oder Weisungen), Organisations- und Informationssicherheitskonzepte bleibt der Raum zwischen diesen Leitplanken leer, und die Wahrung der Persönlichkeitsrechte der betroffenen Personen kann nicht sichergestellt werden. Gefordert sind damit nicht nur die Vertreterinnen und Vertreter der Legislative, sondern insbesondere die Departementsleitungen bezüglich der Gesamtverantwortung und -mentalität innerhalb des Kantons sowie die jeweiligen Dienststellen- oder Abteilungsleiterinnen und -leiter, was die konkrete Ausgestaltung der Organisation ihrer Einheiten angeht. Auf der Ebene der Departementsleitungen ist das Stichwort hierbei unzweifelhaft «IT-Governance»[54], während es für die Dienstellen- und Abteilungsleitungen «gelebte Verantwortlichkeit» ist:

[Rz 68] IT-Governance ist ein strategisches Gesamtkonzept, das auf einer *übergeordneten* Ebene beschreibt, wie die IT innerhalb einer Organisation (d.h. in der öffentlichen Verwaltung entweder in einer Dienststelle, einem Departement oder gar im gesamten Kanton) gesteuert werden soll. Unter anderem legt die IT-Governance fest, wie beispielsweise die Ausrichtung der IT am operativen Geschäft sichergestellt werden soll, wie die Verantwortlichkeiten geregelt werden, wie der Umgang mit Risiken aussehen soll und wie sichergestellt werden soll, dass die Ziele auch erreicht werden. So definiert beispielsweise die Norm ISO 38500[55] als eines der für die IT-Governance relevanten Frameworks folgende Bereiche für die IT-Governance: Verantwortung (Responsibility), Strategie (Strategy), Beschaffung (Acquisition), Leistung (Performance), Regelkonformität (Conformance) und den Faktor Mensch (Human behaviour). Eines der Herzstücke von COBIT, einem weiteren prominenten Rahmenwerk für IT-Governance, ist eine Zielkaskade, welche ausgehend von den Anspruchsgruppen-Treibern über die Unternehmensziele der Organisation (Strategie) und die IT-Ziele (IT-Strategie) zu den Enabler-Zielen (Umsetzung) einen Zusammenhang abzubilden versucht. Mit dem von COBIT gewählten Vorgehen soll erreicht werden, dass relevante und greifbare Ziele und Zielvorgaben auf verschiedenen Zuständigkeitsebenen vorhanden sind und deren Abhängigkeit und Zusammenhang klar ersichtlich ist. Beiden, ISO 38500 und COBIT, ist gemein, dass die Verantwortung für den Einsatz und den Nutzen der IT nicht ausschliesslich dem IT-Verantwortlichen (CIO) oder den IT-Managern zugeordnet wird, sondern eben auch den jeweiligen Führungsgremien bzw. -stellen.

[Rz 69] Diese Vorgaben sind nicht projekt- oder applikationsbezogen, sondern eben idealerweise (departements-)übergreifend. Sie sind bei der Ausarbeitung konkreter Vorgaben für die jeweiligen Dienststellen im Sinne einheitlicher Standards und Minimalvorgaben zu berücksichtigen – im Falle der drei vorangehend erläuterten Technologien würde dies bedeuten, dass die von der Kantonsregierung beispielsweise bezüglich des Beschaffungswesens oder der Verantwortlichkeiten verabschiedeten Kriterien bereits in der jeweiligen Projektphase berücksichtigt werden und bei der Ausarbeitung der spezifischen Organisationsreglemente, Berechtigungskonzepte und Nutzervorgaben einfliessen müssen.

[Rz 70] Eine seriöse Umsetzung der neuen IT-Governance muss unbestrittenermassen als eine der wichtigsten Aufgaben der kantonalen Verwaltung in den kommenden Jahren betrachtet werden: Hierbei wird dem jeweiligen Gesamt-Regierungsrat eine zentrale Rolle zukommen. Er trägt nicht nur die Verantwortung für die strategischen Vorgaben, die Sicherstellung deren Umsetzung sowie

54 Dieser Abschnitt stammt im Wesentlichen aus dem Tätigkeitsbericht des Jahres 2014 des Datenschutzbeauftragten des Kantons Basel-Stadt, abrufbar unter http://www.dsb.bs.ch/dms/dsb/download/publikationen/taetigkeitsberichte/2014_taetigkeitsbericht/TB-DSB2014.pdf.

55 ISO/IEC 38500:2008 Corporate governance of information technology.

ein angemessenes Risikomanagement, letztlich ist er das oberste Führungsgremium der Exekutive und vor allem auch das Bindeglied zwischen den Departementen. Die Vorgaben, was zentral und was dezentral behandelt werden soll, kann letztlich nur der Gesamt-Regierungsrat vorgeben und die zielführende Durchsetzung sicherstellen.

[Rz 71] Gerade für eine föderal strukturierte Organisation wie eine kantonale Verwaltung ergeben sich bezüglich der Verantwortlichkeiten spezielle Herausforderungen. IT-Governance in der öffentlichen Verwaltung ist ein Balanceakt zwischen föderalen Strukturen und zentralen Vorgaben. Dieser Herausforderung müssen sich künftig alle öffentlichen Verwaltungen der Schweiz stellen – sie werden über kurz oder lang um die Verabschiedung einer IT-Governance nicht mehr herumkommen.

[Rz 72] Solange die IT-Governance jedoch noch in den Kinderschuhen steckt, muss umso grösseres Augenmerk auf eine klare Regelung der Verantwortlichkeiten innerhalb der Amtsstellen gelegt werden: Immerhin legen die (Informations- und) Datenschutzgesetze[56] klar fest: «Die Verantwortung für den Umgang mit Informationen trägt dasjenige öffentliche Organ, das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet.» Es muss daher zwingend für alle bearbeiteten Informationen geklärt sein, wie diese Verantwortung ausgestaltet ist. Um auf das Beispiel der digitalen Nummernschilderkennung zurückzukommen: Wer darf das Fahrzeug fahren, wer ist für die Erstellung der Listen der säumigen Steuerzahlerinnen und zahler verantwortlich, wer für das Update der Datenbank im Fahrzeug bzw. des USB-Sticks?

[Rz 73] Wer neue Technologien in den Verwaltungsalltag einbinden möchte, darf nicht nur die Vorteile in den Vordergrund stellen, sondern muss sich auch die Risiken vor Augen führen, sie gegenüber den Vorteilen abwägen und dann bewusst einen Entscheid fällen, ob die jeweilige Technologie eingesetzt werden kann und soll – und wenn ja, welche organisatorischen Massnahmen zu treffen sind, um das Risiko von Persönlichkeitsverletzungen zu minimieren, und welche Restrisiken in Kauf genommen werden (müssen). Diese übergeordnete Verantwortung kann nicht bei einzelnen Mitarbeiterinnen und Mitarbeitern liegen, sie obliegt der jeweiligen Dienstellen-, Abteilungs- oder Bereichsleitung.

[Rz 74] Verantwortlichkeiten müssen aber auch ernstgenommen, ja «gelebt» werden – es genügt nicht, wenn ein sorgfältig erarbeitetes Organisationsreglement oder Weisungen in einer Schublade verstauben, wenn jede und jeder etwas macht, weil «man es einfach immer schon so gemacht hat» oder wenn sich letztendlich niemand für etwas verantwortlich fühlt. Es ist daher an den jeweiligen Leitungspersonen, den Mitarbeiterinnen und Mitarbeitern *ihre* Verantwortung bewusst zu machen, nämlich die alltägliche Verantwortung im Umgang mit Personendaten, welche durch den Einsatz von technischen Hilfsmitteln nicht etwa schwindet, sondern eher an Bedeutung gewinnt.

V. Fazit

[Rz 75] Die Technik galoppiert in bislang ungeahnte Gefilde und bietet mit jedem Entwicklungsschritt neue Möglichkeiten: Schnellere Datenverarbeitung, grössere Speicherkapazitäten, bessere Verknüpfungsmöglichkeiten, eine Vereinfachung der Arbeitsabläufe.

[Rz 76] Diesen Entwicklungen kann und soll sich die Verwaltung nicht entziehen. Dabei darf jedoch

56 Vgl. dazu nur Art. 16 DSG, § 6 IDG/BS, Art. 17 des Freiburger Gesetzes vom 25. November 1994 über den Datenschutz (RSF 17.1) oder aber Art. 11 des Jurassischen loi du 15 mai 1986 sur la protection des données à caractère personnel (RSJU 170.41).

nicht ausser Acht gelassen werden, dass diese Vereinfachungen des Arbeitsalltags – selbst wenn sie keine neuen Möglichkeiten bieten, sondern schlicht einen Ersatz der vormals von Mitarbeiterinnen und Mitarbeitern vorgenommenen Handlungen darstellen – auch ihre Risiken und neue Fragestellungen mit sich bringen. Sei dies, weil die Fingierung der öffentlichen Kenntnisnahme von einer Betreibungsurkunde plötzlich nicht mehr nur innerhalb einer Stadt sondern mit der Publikation im Internet weltweit erfolgt, sei dies, weil mit der Digitalisierung von Archivalien und dem damit verbundenen weltweiten Zugang zu den Dokumenten ein neues Archiv-Benutzerkonzept erstellt und die Wahrung der Schutzfristen neu gesichert werden muss, oder sei es, weil mit dem automatischen Nummernschildabgleich nicht nur ein Generalverdacht gegenüber sämtlichen in einem Quartier geparkten Fahrzeuge konstruiert wird, sondern weil auch weitaus einfacher und längerfristiger registriert werden kann, welches Fahrzeug wann wo geparkt war, als dies bei von Mitarbeiterinnen und Mitarbeitern der Polizei durchgeführten Stichprobenkontrollen der Fall ist.

[Rz 77] Diese Probleme sind nicht gänzlich unlösbar, nur lösen sie sich weder von selbst noch sind sie so geringfügig, dass sie ohne weiteres in Kauf genommen werden sollten. Kurzum: Die öffentlichen Stellen müssen sich ihrer Verantwortung im Umgang mit technischen Mitteln, die den Verwaltungsalltag ergänzen und vereinfachen sollen, bewusst werden, und entsprechend agieren. Dabei ist es nicht zwingend, dass gänzlich neue Rechtsgrundlagen geschaffen werden – im Falle des digitalen Archivs dürfte es unter Umständen genügen, wenn die Bestimmungen zu den Schutzfristen angepasst und der digitale Zugang neu geregelt werden. Ähnliches gilt für die digitalen Amtsblätter: Die Publikationsgesetze müssen freilich die jeweilige Publikationsform festlegen. Ob die formell-gesetzliche Festlegung von Publikations-Zeiträumen sinnvoll ist oder ob nicht auch eine Verordnung genügen würde, kann offen bleiben – es geht dabei in Anbetracht des Umstandes, dass einmal im Internet veröffentlichte Daten faktisch ohnehin nicht mehr gelöscht werden können, auch mehr um ein bewusstes Committment der Verwaltung zum Schutz der Persönlichkeitsrechte der betroffenen Personen und zur Minimierung der Risiken so weit als (technisch) möglich. Unumgänglich scheint hingegen beispielsweise die Schaffung einer gesetzlichen Grundlage für den automatisierten Abgleich von Nummernschildern im Rahmen von Verkehrskontrollen.

[Rz 78] Allein die Schaffung aktueller gesetzlicher Grundlagen genügt jedoch nicht, um den Herausforderungen für die Informationssicherheit zu begegnen. Vielmehr bedarf es kantonaler IT-Strategien, sorgfältig ausgearbeiteter und regelmässig evaluierter Informationssicherheitskonzepte, Berechtigungskonzepte und damit verbunden klarer Zuweisungen der Verantwortlichkeiten.

[Rz 79] Damit wird deutlich: Der rasende Galopp des technischen Fortschritts ist durchaus zähm- und lenkbar. Die Verantwortung dafür tragen aber nicht nur die Mitglieder der Legislative im Rahmen der Gesetzgebung, sondern insbesondere auch die Gesamtregierung bezüglich der Festlegung einer kantonsweiten IT-Strategie (IT-Governance), die Dienststellenleitungen bezüglich der Organisation ihrer Verwaltungseinheiten und der damit verbundenen Verantwortung sowie letztendlich jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter als Reiterinnen und Reiter, als Nutzerinnen und Nutzer der neuen technischen Möglichkeiten.

Dr. iur. Sandra Husi-Stämpfli, LL.M. ist stellvertretende Datenschutzbeauftragte des Kantons Basel-Stadt.