GUTACHTEN
ZUR DATENPORTABILITÄT SOWIE ZU REGELUNGEN BETREFFEND DIE WIEDERVERWENDUNG VON DATEN

Avis 17-063

Lausanne, den 15. Februar 2018

INHALTSVERZEICHNIS

I. HINTERGRUND UND FRAGESTELLUNG

1. Hintergrund

Le 22 mars dernier, le Conseil fédéral a défini les objectifs prioritaires pour une politique suisse des données cohérente et tournée vers l'avenir (voir le communiqué de presse : https://www.uvek.admin.ch/uvek/fr/home/detec/medias/communiques-de-presse.msg-id-66068.html). Dans ce cadre, le DFJP est chargé d'étudier *de lege lata* et *de lege ferenda* certaines questions spécifiques ayant trait à la portabilité des données personnelles et à la réutilisation de données (personnelles ou non) à des fins privées ou publiques.

2. Fragen

[L'Office fédéral de la justice souhaite] que l'ISDC effectue une étude de droit comparé dans les pays suivants : France, Allemagne, Suède, Japon et Etats-Unis. Le droit de l'Union européenne devra également être pris en compte dans la mesure où il a eu une influence sur le droit des Etats membres visés par la présente étude. Cette liste peut être modifiée ou complétée si l'équipe de l'ISDC a connaissance d'autres Etats ayant légiféré sur les points mentionnés ci-dessous.

Les points à examiner seront les suivants :

1) Existence d'un droit à la portabilité des données personnelles dans les pays étudiés : Le droit des Etats concernés permet-il aux personnes concernées d'exiger du responsable du traitement qu'ils leur fournissent leurs données personnelles dans un format structuré, couramment utilisé et lisible par machine, et leur donnent le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ? Quelles sont les données concernées par le droit à la portabilité des données (portée du droit à la portabilité des données) ? Cas échéant, l'introduction d'un droit à la portabilité des données a-t-elle provoqué des problèmes juridiques particuliers ?

Au cas où il n'existerait pas de droit à la portabilité des données *stricto sensu*, le droit en vigueur des Etats concerné permet-il de répondre aux questions suivantes :

A) La personne concernée peut-elle exiger d'un tiers qui a collecté et traité des données à son sujet qu'il les lui remette à des fins de partage ou de réutilisation, sans que le tiers puisse s'y opposer ?

B) La personne concernée a-t-elle le droit de réutiliser et de partager le résultat ou les données anonymisées qui résultent du traitement (p. ex profil établi sur la base d'un algorithme) ?

L'étude devra également porter sur les deux points suivants :

2) Possibilité pour l'organisme qui crée un contenu digital d'autoriser ou de limiter l'utilisation ou la réutilisation des données par un tiers (par ex. un concurrent) : Les règles relatives au contrat de licence permettent-elles de céder à titre temporaire des données numériques à autrui ? Si oui, dans quelle mesure ? De quelle protection peut bénéficier une entreprise qui crée un contenu digital qui n'est pas couvert par le droit de la propriété intellectuelle (p. ex : base de de données comprenant des données scientifiques ou financières) face à un concurrent qui souhaiterait réutiliser ce contenu sans en demander l'autorisation ? Dans quelle mesure les règles relevant du droit de la concurrence sont-elles applicables à une telle situation ?

3) Obligation pour des personnes physiques ou morales relevant du droit privé de donner accès à l'Etat à des données en leur possession en vue d'une réutilisation : Dans quel cas une obligation est-elle prévue ? A quelle fin l'Etat est-il autorisé à réutiliser les données qui lui ont été remises ?

Die dritte Frage wird auf allfällige allgemeine Verpflichtungen sowie Verpflichtungen in den Bereichen öffentliche Gesundheit und Statistik beschränkt.

3. Vorbemerkungen

Dieser Bericht enthält die vollständigen Länderberichte für Deutschland, Frankreich, Schweden und Japan. Der Bericht zu den USA behandelt lediglich den Aspekt der Datenportabilität und der Verpflichtung zur Gewährung des Zugangs an den Staat, derjenige zur EU enthält neben dem Recht auf Datenportabilität eine Übersicht zur Gewährung von Nutzungsrechten.

II. ANALYSE

A. EU

1. Datenportabilität

1.1. Vorliegen eines Rechts auf Datenportabilität

Art. 20 der EU Datenschutz-Grundverordnung 2016/679 (DSGVO)[1], welche am 25. Mai 2018 die EU-Datenschutzrichtlinie 95/46/EG ersetzen wird und die nationalen Datenschutzgesetze weitgehend obsolet machen wird, sieht das Recht auf Datenübertragbarkeit vor. Dieses Recht soll der betroffenen Person die «Kontrolle über 'ihre' personenbezogenen Daten zurück[..]geben»[2] Daten. Es hat nicht nur eine Berechtigung im Datenschutz (und damit im Konsumentenschutz), sondern hat auch eine bedeutende wettbewerbsrechtliche Funktion.[3]

Das Recht gilt nicht für Datenbearbeitung, welche für die Wahrnehmung einer im öffentlichen Interesse stehenden oder in Ausübung öffentlicher Gewalt erfolgenden Aufgabe (Art. 20 Abs. 3 2. Satz DSGVO).

Das Recht beinhaltet zunächst eine Art **Herausgabeanspruch**, der über das Zugangverschaffen hinausgeht,[4] auch wenn es sich um eine Art Auskunftsanspruch handelt. Die Daten müssen in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden. Dies ist insbesondere für die Herausgabe von durch Plattformanbieter im Internet bearbeitete Daten relevant, wenn auch das Recht allgemeiner ausgestaltet ist. Zweitens sieht die DSGVO aber auch einen Anspruch auf die **behinderungsfreie Übermittlung** der Daten an einen anderen Verantwortlichen vor, wobei diese Übermittlung auch direkt erfolgen kann, soweit dies technisch machbar ist (Art. 20 Abs. 2 DSGVO).

Damit die oben erwähnten Ansprüche gegeben sind, müssen die betreffenden Daten **von der betroffenen Person bereitgestellt** worden sein, d.h. die Person muss sie aktiv und wissentlich zur Verfügung gestellt haben,[5] und es muss sich um **personenenbezogene** Daten über die betroffene Person handeln. Die Datenverarbeitung muss **mit der Einwilligung** der betroffenen Person erfolgen oder auf der Grundlage eines Vertrags, und die Datenbearbeitung muss mit einem automatisiertem Verfahren erfolgen, insbesondere durch Computersysteme. Bei einer manuellen Bearbeitung gilt der Anspruch also nicht. Kontrovers diskutiert wird insbesondere die Frage, ob und wie weit Daten, welche durch die Inanspruchnahme einer Dienstleistung generiert werden (insbesondere durch den Gebrauch einer Dienstleistung, z.B. der Suchverlauf, Verkehrsdaten, Ortsdaten), ebenfalls darunter fallen. Gemäss der «Artikel 29 Datenschutzgruppe», einer gemäss Richtlinie 95/46/EG eingesetzte unabhängige Beratungsinstanz der Europäischen Kommission, die sich aus Vertretern der nationalen

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

[2] Piltz in P. Gola, Datenschutz-Grundverordnung VO (EU) 2016/679, N 3 ad Art. 20, mit Hinweisen.

[3] G. Sydow, Europäische Datenschutzgrundverordnung, Beck 2017, N 1 ad Art. 20.

[4] Piltz, zit., N 8 ad Art. 20.

[5] Piltz, zit., N 14 ad Art. 20.

Aufsichtsbehörden und je einem Vertreter der EU-Kommission und des EU-Datenschutzbeauftragten zusammensetzt, sind diese Daten ebenfalls erfasst.[6] Diese Auslegung wurde jedoch kritisiert.[7]

Schliesslich darf das Herausgabe- und Übermittlungsrecht[8] die **Rechte und Freiheiten** anderer Personen nicht beeinträchtigen (Art. 20 Abs. 4 DSGVO). Damit erlaubt das Recht auf Datenportabilität insbesondere nicht die Herausgabe von Daten, welche (auch) andere Personen betreffen.

1.2. Rückforderungsrecht

Das Rückforderungsrecht ist im Recht auf Datenportabilität enthalten (s. dazu oben, 1.).

1.3. Wiederverwendungsrecht der anonymisierten Daten

Das Recht auf Datenportabilität betrifft nur **personenbezogene Daten**. Es betrifft zudem (wie oben unter 1. erwähnt) lediglich die von der betroffenen Person **bereitgestellten Daten**. Daten, welche durch die Verarbeitung erzeugt worden sind (z.B. eine Beurteilung der Gesundheit, eine Kreditwürdigkeitsbeurteilung, ein Persönlichkeitsprofil), sind deshalb nicht erfasst.[9]

2. Gewähren von Nutzungsrechten an digitalen Inhalten

2.1. Schutz von Datenbanken

In der EU wurde bereits 1996 mit der Richtlinie 96/6/EG[10] ein spezifischer Schutz für **Ersteller von Datenbanken** eingeführt. Die Richtlinie enthält im Wesentlichen zwei Schutzmechanismen: die Ausweitung des Urheberrechtsschutzes auf gewisse Datenbanken sowie ein sui generis Recht, welches an weniger strengere Anforderungen geknüpft ist.

Urheber von Datenbanken, «die aufgrund der Auswahl oder Anordnung des Stoffes eine eigene geistige Schöpfung»[11] darstellen, werden **urheberrechtlich** geschützt. Die Vervielfältigung, Übersetzung, öffentliche Verbreitung oder Aufführung ist damit grundsätzlich nur mit Zustimmung des Urhebers möglich (Art. 5 RL 96/9/EG). Die Mitgliedstaaten können Ausnahmen vorsehen, z.B. die Benutzung der Datenbank zu Zwecken der wissenschaftlichen Forschung (Art. 6 RL 96/9/EG)).

Hersteller einer Datenbank, zu deren Erstellung «eine in qualitativer oder quantitativer Hinsicht wesentliche Investition erforderlich» ist, erhalten ein ***sui generis* Schutzrecht**. Dies gibt dem Hersteller das Recht, die Entnahme oder Weiterverwendung «der Gesamtheit oder eines in qualitativer oder quantitativer Hinsicht wesentlichen Teils» des Inhalts grundsätzlich zu untersagen (Art. 7 Richtlinie 96/9/EG). Auch hier bestehen Ausnahmen, z.B. die Entnahme zum Zweck der wissenschaftlichen Forschung (Art. 9 RL 86/9/EG). Dieses Schutzrecht ist auf 15 Jahre beschränkt (Art. 10 RL 96/9/EG).

---

[6] Article 29 Date Protection Working Party, Guidelines on the right to data portability, angenommen am 13.12.2016, Stand 05.04.2017, S. 10.

[7] S. D. Meyer, European Commission, experts uneasy over WP29 data portability interpretation, 25.04.2017, verfügbar unter https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/.

[8] Die deutsche Fassung verweist in Art. 20 Abs. 4 DSGVO auf Art. 20 Abs. 2, die anderen sprachlichen Fassungen jedoch auf Abs. 1, so dass davon ausgegangen werden muss, dass der Verweis richtigerweise auf Abs. 1 erfolgt; s. Sydow, N 18 f ad Art. 20.

[9] Article 29 Date Protection Working Party, Guidelines on the right to data portability, angenommen am 13.12.2016, Stand 05.04.2017, S. 10.

[10] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11.03.1996 über den rechtlichen Schutz von Datenbanken.

[11] Art. 3 Richtlinie 96/9/EG.

Die Richtlinie 96/9/EG wird aktuell von der Europäischen Kommission **evaluiert**.[12] Es bestehen allerdings keine klaren Anzeichen, ob und in welchen Belangen Änderungen der Richtlinie vorgeschlagen werden. Eine frühere Evaluation führte trotz Zweifeln an der Effektivität der Richtlinie zu keinen Änderungen.[13]

2.2. Weitere Regelungen zur Übertragung von Nutzungsrechten

Die EU ist zwar bestrebt, die digitale Wirtschaft durch die Vereinfachung der grenzüberschreitenden Zirkulation der Daten zu vereinfachen.[14] Das Recht der Europäischen Union enthält abgesehen vom Immaterialgüterrecht (s. 2.1.) keine allgemeinen umfassenden Schutzbestimmungen für Inhaber oder Ersteller von Daten. Drei Regelungsbereiche berühren aber die diesbezüglich anwendbare rechtliche Regelung: Konsumentenschutz, Datenschutz und Wettbewerbsrecht.

Im Bereich des **Konsumentenschutzes** sieht die Richtlinie 2011/83/EU[15] spezifische Schutzvorschriften bei «Verträgen über digitale Inhalte» vor. Die Sonderregel wird damit begründet, dass für entsprechende Verträge weder die Bestimmungen des Dienstleistungsvertrags noch diejenigen des Kaufvertrags angemessen sind.[16] So sieht die Richtlinie insbesondere ein Widerrufsrecht sowie gewisse Informationspflichten (z.B. über die Funktionsweise des digitalen Inhalts) vor. Die Richtlinie enthält keine weiteren Bestimmungen über «Verträge über die Bereitstellung digitaler Inhalte», so dass diesbezüglich nationales Recht angewendet wird. In Ergänzung zur Richtlinie 2011/83/EU hat die Europäische Kommission 2015 eine Richtlinie «über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte» vorgeschlagen.[17] Diese enthält insbesondere Regelungen über die Rechtsbehelfe der Konsumenten. Der Rat der EU hat im Juni 2017 diesbezüglich eine Grundsatzerklärung abgegeben[18], und der Text wird aktuell im Europäischen Parlament beraten.[19]

Soweit es sich um persönliche Daten handelt, ist die **EU-Datenschutz Grundverordnung** (Verordnung 2013/679/EU) anwendbar. Deren Art. 6 setzt grundsätzlich die Einwilligung oder einen anderen Grund voraus, damit eine Bearbeitung persönlicher Daten zulässig wird. Die Für nicht persönliche Daten besteht kein entsprechender Schutz.

---

12 S. Roadmap der Kommission, Ares(2017)2543859, verfügbar unter https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-2543859_en, sowie die erste Übersicht über die Resultate der öffentlichen Konsultation vom 6.10.2017, verfügbar unter https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-legal-protection-databases.

13 DG Internal Market and Services Working Paper, First evaluation of Directive 96/9/EC on the legal protection of databases, 12.12.2005, verfügbar unter http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf.

14 S. dazu insbesondere der Vorschlag vom 13.09.2017 einer Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, COM(2017)495 final.

15 Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, zur Abänderung der Richtlinie 93/13/EWG des Rates und der Richtlinie 1999/44/EG des Europäischen Parlaments und des Rates sowie zur Aufhebung der Richtlinie 85/577/EWG des Rates und der Richtlinie 97/7/EG des Europäischen Parlaments und des Rates.

16 S. Präambel Ziff. 19 der RL 2011/83/EU.

17 COM(2015) 634 final, Vorschlag vom 09.12.2015.

18 Verfügbar unter http://data.consilium.europa.eu/doc/document/ST-9901-2017-INIT/en/pdf.

19 S. die Verabschiedung im entsprechenden Ausschuss vom 27.11.2017: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2BREPORT%2BA8-2017-0375%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN.

In **wettbewerbsrechtlicher** Sicht besteht soweit ersichtlich kein besonderer Schutz von Daten. Dies liegt insbesondere daran, dass das Lauterkeitsrecht diesbezüglich nicht europäisch harmonisiert ist: «[u]nter welchen Voraussetzungen [neben dem Recht des geistigen Eigentums] auch ein lauterkeitsrechtlicher Schutz vor Produktnachahmungen zu gewähren ist, wird in den Mitgliedstaaten unterschiedlich beurteilt.»[20] Rechtliche Regelungen werden nicht im Sinne eines Schutzes an Daten, sondern im Sinne eines Zugangs zu Daten diskutiert. So können tatsächliche Zugangsbeschränkungen zu Daten kartellrechtlich relevant sein, wenn die Daten «ein unverzichtbarer Inputfaktor für die (potentiellen) Anbieter auf einem dem Datenzugang nachgelagerten Markt» sind, d.h. die Konkurrenten «müssen von dem Zugang zu diesen Daten abhängig sein, um dort tätig werden zu können» (*Essential Facilities* Doktrin des EuGH).[21]

B. DEUTSCHLAND

1. Datenportabilität

1.1. Vorliegen eines Rechts auf Datenportabilität

Im deutschen Recht besteht soweit ersichtlich unter dem aktuell geltenden Datenschutzrecht kein Recht auf Datenportabilität.[22]

1.2. Rückforderungsrecht

S. oben, 1.1.

1.3. Wiederverwendungsrecht des Ergebnisses oder der anonymisierten Daten

Das deutsche Recht enthält soweit ersichtlich kein Wiederverwendungsrecht.

2. Gewähren von Nutzungsrechten an digitalen Inhalten

§ 312f Absatz 3 Bürgerliches Gesetzbuch enthält eine Legaldefinition von digitalen Inhalten. Demnach sind digitale Inhalte „**Daten, die in digitaler Form hergestellt und bereitgestellt werden**". Dazu gehören unter anderem Computerprogramme, Anwendungen (*Apps*), Spiele, Musik- und Videodateien oder Texte.[23] Es ist unerheblich, ob die Daten heruntergeladen, gespeichert und dann sichtbar gemacht werden oder während des Herunterladens in Echtzeit sichtbar gemacht werden (*Streaming*).[24] Die Bestimmung im Bürgerlichen Gesetzbuch präzisiert die Anwendung von Konsumentenschutzbestimmungen (insbesondere bezüglich des Widerrufsrechts) bei Verträgen über die Lieferung von digitalen Inhalten.

---

20 C. Busch, Lauterkeitswrecht in Europa: Acquis communautaire, in M. Schmidt-Kessel & S. Schubmehl, Lauterkeitsrecht in Europa, Mènchen 2011, S. 1 ff., S. 23.

21 Deutsches Bundeskartellamt, Big Data und Wettbewerb, Schriftenreihe «Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft», Nr. 1, Oktober 2017, S. 10, mit Hinweisen auf die Rechtsprechung des EuGH i.S. „IMS Health", C-418/01, 29.04.2004; "Bronner", C-7/97, 26.11.1998, und "Microsoft", T-201/04, 17.09.2007.

22 S. von Lewinski, in H.A. Wolff & S. Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 22. Ed., München 2017, Art. 20 DS-GVO, Rn. 1.

23 S. Martens, in H.G. Bamberger *et al.*, Beck'scher Onlinekommentar BGB (Hrsg.), 43. Aufl., München 2017, § 312f, Rn. 12.

24 C. Gründeberg, in O. Palandt (Hrsg.), Bürgerliches Gesetzbuch, 76. Aufl., München 2017, § 312f, Rn. 4.

In Deutschland sind digitale Inhalte in erster Linie durch das Urheberrechtsgesetz und das Patentgesetz geschützt.[25] Der im europäischen Recht vorgesehene Schutz **des Datenbankherstellers** wurde im Urheberrechtsgesetz umgesetzt (insbesondere § 87 a bis § 87 e).

Wie oben erwähnt sehen sowohl das Urheberrecht[26] wie auch das Patentrecht[27] vor, dass **Nutzungsrechte an digitalen Inhalten** vergeben werden können. Diese Nutzungsrechte an immateriellen Gütern werden vorwiegend durch Lizenzverträge[28] erteilt. **Lizenzverträge** sind zwar vom Gesetzgeber anerkannt[29], jedoch bis heute nicht gesetzlich normiert.[30]

Eine **Weiterveräusserung der Lizenz** wie auch die Vergabe von Unterlizenzen werden im Urheberrecht (§§ 34 und 35 UrhG) vorgesehen. Auch bei den Patentrechten ist sowohl eine Übertragung der Lizenz als auch die Vergabe von Unterlizenzen grundsätzlich möglich. Da dazu entsprechende gesetzliche Bestimmungen fehlen, sind in erster Linie die Vereinbarungen der Parteien entscheidend.[31]. Unklar scheint dabei die Anwendung des sogenannten **Erschöpfungsgrundsatzes** zu sein, wonach das Verbreitungsrecht des Rechtsinhabers beschränkt wird, indem der Rechtsinhaber durch die Erstverbreitung das ihm vom Gesetz eingeräumte ausschliessliche Verwertungsrecht ausgenutzt und damit verbraucht hat.[32].

Ist ein immaterialrechtlicher Sonderrechtsschutz nicht oder nicht mehr gegeben, so steht die Benutzung der Leistung anderer für die eigene gewerbliche Betätigung grundsätzlich frei.[33] Auch

---

25 Der Designschutz nach dem Designgesetz (DesignG) und der Markenschutz nach dem Markengesetz (MarkenG) werden in diesem Länderbericht nicht behandelt.

26 §§ 31 ff. Urheberrechtsgesetz (UrhG).

27 § 15 Patentgesetz (PatG).

28 L. Pahlow, in J.D. Harke (Hrsg.), Beck-online. GROSSKOMMENTAR, Stand 01.09.2017, § 581 BGB, Rn. 234.

29 Insbesondere § 15 Abs. 2 und 3 Patentgesetz (PatG).

30 L. Pahlow, in J.D. Harke (Hrsg.), Beck-online. GROSSKOMMENTAR, Stand 01.09.2017, § 581 BGB, Rn. 200 ff.

31 L. Pahlow, in J.D. Harke (Hrsg.), Beck-online. GROSSKOMMENTAR, Stand 01.09.2017, § 581 BGB, Rn. 323; Bei digitalen Inhalten wird vom Lizenzgeber häufig ein einfaches, nicht übertragbares Nutzungsrecht zum ausschliesslich persönlichen Gebrauch eingeräumt und die Weiterverbreitung untersagt. Damit wollen die Lizenzgeber verhindern, dass digitale Inhalte ohne Qualitätsverlust und zu fast keinen Kosten in praktisch beliebiger Stückzahl vervielfältigt und an Dritte weitergegeben werden können. (s. J. Marly & A.-L. Wirz, Die Weiterverbreitung digitaler Güter, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2017, S. 16).

32 J. Marly & A.-L. Wirz, Die Weiterverbreitung digitaler Güter, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2017, S. 16. Dieser Grundsatz ist in Art. 4 Abs. 2 der InfoSoc-Richtlinie 2001/29/EG, Art. 9 Abs. 2 der Vermiet- und Verleih-Richtlinie 2006/115/EG sowie §§ 17 Abs. 2 und 69c Nr. 3 UrhG vorgesehen; Für *Software* hat der Europäische Gerichtshof in einem grundlegenden ***UsedSoft*-Entscheidung** zum Gebrauchtsoftwarehandel die Anwendung des Erschöpfungsgrundsatz auch für online übermittelte Programmkopien bejaht. der Europäische Gerichtshof seine Entscheidung ausschliesslich auf die urheberrechtlichen Sondervorschriften für Computerprogramme stützte, kann das Urteil nicht ohne Weiteres auf andere digitale Güter übertragen werden. Jüngere Entscheide deutscher Gerichte verneinen ausdrücklich eine Übertragbarkeit dieser Rechtsprechung auf andere digitale Inhalte (Oberlandesgericht (OLG) Hamm, Urteil vom 15.05.2014 – 22 U 60/13; OLG Stuttgart, Urteil vom 03.11.2011 – 2 U 49/11. Zum einen wurde dies mit der Spezialität der Sondervorschriften für Computerprogramme begründet, zum anderen damit, dass dem Verbraucher geläufig sei, dass die Verkehrsfähigkeit eines heruntergeladenen digitalen Gutes eingeschränkt sei).

33 A. Nordemann, in H.-P. Götting & A. Nordemann (Hrsg.), UWG, 3. Aufl., Baden-Baden 2016, § 4, Rn. 3.3.

herrscht wettbewerbsrechtlich grundsätzlich Nachahmungsfreiheit.[34] Das **Wettbewerbsrecht** greift nur dann ein, wenn und soweit die Benutzung dem Prinzip des freien Leistungswettbewerbs zuwiderläuft.[35] Unter Umständen können digitale Inhalte also (auch) wettbewerbsrechtlich geschützt sein. Dazu kommt vorwiegend ein Nachahmungsverbot in Betracht, wenn die Nachahmung eine vermeidbare Herkunftstäuschung herbeiführt[36], die Wertschätzung der nachgeahmten Ware oder Dienstleistung unangemessen ausnützt oder beeinträchtigt[37] oder unredlich Kenntnisse oder Unterlagen erlangt werden[38] oder auch wenn der Mitbewerber gezielt behindert wird[39].

Die Rechtsprechung und die Lehre gingen lange Zeit von der sogenannten Vorrangthese aus: Der Sonderrechtsschutz (wie zum Beispiel das Urheberrecht und der Patentschutz) habe grundsätzlich Vorrang vor dem ergänzenden wettbewerbsrechtlichen Leistungsschutz.[40] Diese Vorrangthese wurde zwischenzeitlich in der Rechtsprechung und der Lehre immer mehr eingeschränkt.[41] Gegen den Vorrang des Sonderrechtsschutzes und für einen **Gleichrang** des lauterkeitsrechtlichen Nachahmungsschutzes spricht vor allem, dass der Sonderrechtsschutz und der lauterkeitsrechtliche Nachahmungsschutz unterschiedliche Schutzzwecke, unterschiedliche Voraussetzungen und unterschiedliche Rechtsfolgen haben.[42] Daher können – unabhängig vom Bestehen von Ansprüchen aus einem Sonderschutzrecht – Ansprüche aus wettbewerbsrechtlichem Leistungsschutz gegeben sein, wenn besondere Begleitumstände vorliegen, die ausserhalb des gesetzlichen Tatbestands liegen.[43] Man kann insoweit auch von Anspruchskonkurrenz sprechen.[44]

Betreffend dem Urheberrecht gilt, dass nach der neueren Rechtsprechung[45] wettbewerbsrechtliche Ansprüche unabhängig vom Bestehen urheberrechtlicher Ansprüche gegeben sein können, wenn besondere Begleitumstände vorliegen, die ausserhalb der Sonderschutztatbestände des Urheberrechts liegen.[46] Der lauterkeitsrechtliche Nachahmungsschutz ergänzt daher nicht das Sonderrecht, sondern steht grundsätzlich gleichrangig daneben.[47]

Auch für das Patentrecht gilt, dass unabhängig vom Bestehen von patentrechtlichen Ansprüchen Ansprüche aus lauterkeitsrechtlichem Leistungsschutz gegeben sein können, wenn besondere Begleitumstände vorliegen, die ausserhalb des patentrechtlichen Tatbestands liegen.[48] Ist der Patentschutz für ein bestimmtes Merkmal des Produkts abgelaufen, welches diesem wettbewerbliche

---

34 A. Nordemann, in H.-P. Götting & A. Nordemann (Hrsg.), UWG, 3. Aufl., Baden-Baden 2016, § 4, Rn. 3.3; T. Sambuc, in H. Harte-Bavendamm & F. Henning-Bodewig (Hrsg.), UWG, 4. Aufl., München 2016, § 4 Nr. 3, Rn. 21.

35 A. Nordemann, in H.-P. Götting & A. Nordemann (Hrsg.), UWG, 3. Aufl., Baden-Baden 2016, § 4, Rn. 3.21.

36 § 4 Abs. 3 Buchst. a UWG.

37 § 4 Abs. 3 Buchst. b UWG.

38 § 4 Abs. 3 Buchst. c UWG.

39 § 4 Abs. 4 UWG.

40 H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.6.

41 H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.6.

42 H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.6a; so auch der Bundesgerichtshof (BGH), Urteil vom 24.01.2013 – I ZR 136/11 (Regalsystem); BGH Urteil vom 22.01.2015 – I ZR 107/13 (Exzenterzähne).

43 Bundesgerichtshof (BGH), Urteil vom 24.01.2013 – I ZR 136/11 (Regalsystem).

44 H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.6a.

45 Bundesgerichtshof (BGH), Urteil vom 01.12.2010 – I ZR 12/08 (Perlentaucher); BGH Urteil vom 12.05.2011 – I ZR 53/10 (Seilzirkus).

46 Dazu gehören die in § 4 Nr. 3 Buchst. a und b und § 4 Nr. 4 genannten Umstände.

47 H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.6a

48 Bundesgerichtshof (BGH) Urteil vom 22.01.2015 – I ZR 107/13 (Exzenterzähne); H. Köhler *et al*., Gesetz gegen den unlauteren Wettbewerb, 35. Aufl., München 2017, § 4, Rn. 3.12.

Eigenart verleiht, so kann gemäss dem Bundesgerichtshof trotzdem ein lauterkeitsrechtlicher Schutz möglich sein. Voraussetzung hierfür ist, dass die konkrete Gestaltung dieses Elements technisch nicht notwendig ist, sondern durch eine frei wählbare und austauschbare Gestaltung, die denselben technischen Zweck erfüllt, ersetzt werden kann, ohne dass damit Qualitätseinbussen verbunden sind.[49]

Die Rechtsfolgen eines Wettbewerbsverstosses sind in den §§ 8 – 10 Gesetz gegen den unlauteren Wettbewerb vorgesehen. Das Gesetz sieht Ansprüche auf Unterlassung und Beseitigung, Schadenersatz und Gewinnabschöpfung vor.[50]

3. Verpflichtung zur Gewährung des Zugangs an den Staat

3.1. Public Health

Um Gefahren für die Gesundheit der Bevölkerung vorzubeugen, bestehen im deutschen Recht Vorschriften, welche abweichend von der für Ärzte und andere Heilberufe geltenden Verschwiegenheitspflicht[51] bestimmte **Meldepflichten** vorsehen. Diese Ausnahmen sind im Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (**Infektionsschutzgesetz**, IfSG)[52] geregelt.

Das Infektionsschutzgesetz listet in § 6 bestimmte **Krankheiten**[53] auf, die meldepflichtig sind, und in § 7 bestimmte **Nachweise von Krankheitserregern**, die gemeldet werden müssen. In beiden Fällen unterscheidet das Gesetz jeweils einerseits zwischen Krankheiten beziehungsweise Nachweisen von Krankheitserregern, bei denen eine **namentliche Nennung der betroffenen Person** erforderlich ist, und andererseits solchen Fällen, in denen eine **nichtnamentliche Meldung** ausreichend ist. Welche Angaben in den jeweiligen Konstellationen zu machen sind, regeln § 9 Infektionsschutzgesetz über die namentliche Meldung und § 10 Infektionsschutzgesetz über die Nichtnamentliche Nennung.

Im Detail hängen die genauen Vorgaben von der jeweiligen Krankheit ab. Im Hinblick auf Daten, die dem jeweiligen Arzt durch den Patienten zur Verfügung gestellt wurden, müssen bei einer **namentlichen Meldung** in jedem Fall folgende Angaben weitergegeben werden:

- Name und Vorname,
- Geschlecht,
- Geburtsdatum,
- Anschrift der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes und, falls abweichend: Anschrift des derzeitigen Aufenthaltsortes und
- Weitere Kontaktdaten.[54]

Darüber hinaus müssen **bei bestimmten Krankheiten** auch weitere Angaben gemeldet werden, wie beispielsweise

- Die wahrscheinliche Infektionsquelle inklusive der zugrunde liegenden Tatsachen,
- Die Tätigkeit in einer Heileinrichtung, in einer Massenunterkunft oder im gastronomischen Bereich,

---

49 Bundesgerichtshof (BGH) Urteil vom 22.01.2015 – I ZR 107/13 (Exzenterzähne).

50 Daneben kommen auch nicht im UWG geregelte Anspruche in Betracht, wie zum Beispiel Bereicherungsansprüche aus § 812 Abs. 1 Bürgerliches Gesetzbuch (BGB).

51 Siehe hierzu beispielsweise § 203 Strafgesetzbuch (StGB).

52 Verfügbar unter http://www.gesetze-im-internet.de/ifsg/index.html (19.12.2017).

53 Erfasst sind der Verdacht auf eine Erkrankung, die Erkrankung selbst oder ein durch die Erkrankung bedingter Todesfall, § 6 Abs. 1 Nr. 2 Infektionsschutzgesetz (IfSG).

54 § 9 Abs. 1 Nr. 1 lit. a)-e), Abs. 2 Nr. 1 lit. a)-e) Infektionsschutzgesetz (IfSG).

- Geburtsstaat, Staatsangehörigkeit und gegebenenfalls Jahr der Einreise nach Deutschland,
- Aufnahme und Entlassung aus einer Heileinrichtung,
- Blut-, Organ, Gewebe- und Zellspenden der letzten sechs Monate sowie
- Der relevante Impfstatus.[55]

Im Rahmen einer **nichtnamentlichen Meldung** hingegen müssen mindestens die folgenden Angaben weitergegeben werden, die der Patient dem Arzt bekanntgegeben hat:

- Geschlecht und
- Monat und Jahr der Geburt.[56]

Darüber hinaus sind **in manchen Fällen** auch die folgenden Daten meldepflichtig:

- Die ersten drei Ziffern der Postleitzahl der Hauptwohnung oder des gewöhnlichen Aufenthaltsortes,
- Die wahrscheinliche Infektionsquelle inklusive der zugrunde liegenden Tatsachen.
- Staat, in dem die Infektion wahrscheinlich erfolgt ist,
- Expositions- und Chemoprophylaxe sowie
- Das fallbezogene Pseudonym der Person, welches aus dem dritten Buchstaben des ersten Vornamens und der Anzahl der Buchstaben des ersten Vornamens sowie dem dritten Buchstaben des ersten Nachnamens und der Anzahl der Buchstaben des ersten Nachnamens besteht.[57]

Gemäss § 8 Infektionsschutzgesetz zur Meldung von meldepflichtigen Krankheiten verpflichtet ist insbesondere der **feststellende Arzt**, in grösseren Einrichtungen auch der **leitende Arzt** und gegebenenfalls der **leitende Abteilungsarzt** oder der **behandelnde Arzt**.[58] Meldungen über Nachweise über Krankheitserreger müssen vom Leiter der Untersuchungsstelle vorgenommen werden.[59] Je nach Krankheiten betrifft die Meldepflicht auch Leiter von Einrichtungen der pathologisch-anatomischen Diagnostik, Tierärzte, Angehörige von Heil- und Pflegeberufen, sofern ihre Berufsausübung eine staatliche geregelte Ausbildung oder Anerkennung erfordert, Leiter von Massenunterkünften sowie Heilpraktiker.[60]

Die Meldung erfolgt bei namentlicher Meldung an das **Gesundheitsamt**, in dessen Bezirk sich der Patient derzeit aufhält oder zuletzt aufhielt.[61] Nichtnamentliche Meldungen von Krankheiten richten sich zwar ebenfalls an das Gesundheitsamt, jedoch an dasjenige, in dessen Bezirk sich die Einrichtung befindet.[62] Das jeweilige Gesundheitsamt übermittelt die verarbeiteten Daten an die zuständige Landesbehörde sowie von dort an das **Robert-Koch-Institut**.[63] Nichtnamentliche Meldungen von Nachweisen über Krankheitserreger werden hingegen direkt an das Robert-Koch-Institut gemeldet.[64] Das Robert Koch-Institut hat die gesetzliche Aufgabe, Konzepte zur Vorbeugung übertragbarer Krankheiten und zur frühzeitigen Erkennung und Verhinderung der Weiterverbreitung von Krankheiten zu entwickeln.[65]

---

55 § 9 Abs. 1 Nr. 1 lit.) f)-h), k)-p). Infektionsschutzgesetz (IfSG).

56 § 10 Abs. 1 Nr. 2 lit. a), b), Abs. 2 Nr. 2, 3 Infektionsschutzgesetz (IfSG).

57 § 10 Abs. 1 Nr. 2 lit. f), Abs. 2 Nr. 1, 4, 9-11 Infektionsschutzgesetz (IfSG).

58 § 8 Abs. 1 Nr. 1 Infektionsschutzgesetz (IfSG).

59 § 8 Abs. 1 Nr. 2 Infektionsschutzgesetz (IfSG).

60 § 8 Abs. 1 Nr. 3-8 Infektionsschutzgesetz (IfSG).

61 § 9 Abs. 4 S. 1 Infektionsschutzgesetz (IfSG).

62 § 10 Abs. 1 S. 1 Infektionsschutzgesetz (IfSG).

63 § 11 Abs. 1 S. 1 Infektionsschutzgesetz (IfSG).

64 § 10 Abs. 2 S. 1 Infektionsschutzgesetz (IfSG).

65 § 4 Abs. 1 S. 1 Infektionsschutzgesetz (IfSG), weitere Informationen unter www.rki.de (19.12.2017).

3.2. Statistische Zwecke

Als Rechtsgrundlage für die Arbeit des **Statistischen Bundesamtes** dient das Gesetz über die Statistik für Bundeszwecke (**Bundesstatistikgesetz**, BstatG).[66] Beim Statistischen Bundesamt handelt es sich um eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Inneren, welches Statistiken für Bundeszwecke methodisch und technisch vorbereitet und weiterentwickelt.[67]

Bundesstatistiken werden grundsätzlich **durch Gesetz angeordnet**. Hierbei dürfen jedoch nur **Wirtschafts- und Umweltstatistiken** mit **Auskunftspflicht** angeordnet werden; andere Bundesstatistiken dürfen lediglich ohne Auskunftspflicht angeordnet werden.[68]

Diese Auskunftspflicht wird in § 15 Bundesstatistikgesetz näher ausgeführt. Demnach muss das die Statistik anordnende Gesetz festlegen, ob und in welchem Umfang eine Auskunftspflicht bestehen soll. Wird eine solche Pflicht angeordnet, so müssen alle natürlichen und juristischen Personen des Privatrechts und des öffentlichen Rechts, Personenvereinigungen, Behörden des Bundes und der Länder sowie Gemeinden und Gemeindeverbände die ordnungsgemäss gestellten Fragen beantworten.[69] **Das Gesetz geht jedoch nicht darauf ein, inwiefern natürliche oder juristische Personen des Privatrechts hierbei auch Daten weitergeben müssen, welche ihnen von Dritten zur Verfügung gestellt wurden.** Unsere Recherche hat auch keine Literatur oder Rechtsprechung zu dieser Frage ergeben. In Anbetracht der detaillierten Vorschriften über den gesetzlich festzulegenden Umfang der Statistik[70] sowie über die Verwendung und Löschung der zur Verfügung gestellten Erhebungs- und Hilfsmerkmale[71] gehen wir jedoch davon aus, dass ein solcher Eingriff in die Rechte Dritter gesetzlich vorgesehen sein müsste.

C. FRANKREICH

1. Datenportabilität

1.1. Vorliegen eines Rechts auf Datenportabilität

Art. 48 des Loi 2016-1312 pour une République numérique vom 07.10.2016 sieht in Ausführung der DSGVO eine Änderung des französischen Verbraucherrechts (*Code de la consommation*) vor, welche am 25. Mai 2018 in Kraft treten wird. Diese Änderung ergänzt das Kapitel zu den Verbraucherverträgen über elektronische Dienstleistungen (contrats de services de communication électronique) um ein Unterkapitel zur Portabilität und Wiedererlangung von Daten (Portabilité et récupération des données). Nach Art. L. 224-42-1 hat der Verbraucher/die Verbraucherin unter allen Umständen ein Recht, die Gesamtheit seiner/ihrer Daten zurückzuerhalten. Dieses Recht betrifft **nicht nur persönliche Daten**, sondern auch andere Daten. Soweit persönliche Daten betroffen sind, ist Art. 20 DSGVO anwendbar.[72] In diesem Zusammenhang wird deshalb auf die Ausführungen unter A. verwiesen. Für die übrigen Daten sieht das französische Recht folgende Regelung vor.

---

66 Verfügbar unter http://www.gesetze-im-internet.de/bstatg_1987/index.html (19.12.2017).

67 § 2 Abs. 1, § 3 Abs. 1 Nr. 1 Bundesstatistikgesetz (BStatG).

68 § 5 Abs. 1 S. 1, Abs. 2 S. 2 Bundesstatistikgesetz (BStatG).

69 § 15 Abs. 1 S. 1, 2 Bundesstatistikgesetz (BStatG).

70 § 9 Bundesstatistikgesetz (BStatG).

71 § 10 Bundesstatistikgesetz (BStatG).

72 Art. L. 224-42-2.-Cette récupération s'exerce conformément aux conditions prévues à l'article 20 du règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE, pour les données ayant un caractère personnel, et à la présente sous-section pour les autres.

Jeder Dienstleistungserbringer muss (unter Vorbehalt des Geschäftsgeheimnisses und des Schutzes von Immaterialgüterrechten) alle von der betroffenen Person «online» gestellten Inhalte sowie die aus der Nutzung generierten und für den Nutzer einsehbaren Daten – sofern sie nicht wesentlich «angereichert» wurden (ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause) – in einer kostenlosen und einfachen Art, durch einmalige Abfrage, wieder «erhaltbar» machen.[73] Gegenstand des Herausgaberechts sind schliesslich auch weitere mit dem Nutzerkonto verbundenen Daten, welche den Wechsel zu einem Anbieter erleichtern und u.a. aufgrund der wirtschaftlichen Wichtigkeit der Dienstleistung, des Wettbewerbs zwischen den Anbietern und des Nutzens für den Verbraucher angebracht sind.[74]

1.2. Rückforderungsrecht

En plus du droit à la portabilité précédemment présenté, un droit à la récupération est prévu dans la loi pour une République numérique (LRN) pour certaines données spécifiques dans un format facilitant leur réutilisation. Tel est le cas pour les informations publiques, les données issues de délégation de service public, les données relatives aux subventions, les données de consommation et de production d'énergie, le répertoire de la CNIL de l'ensemble des traitements qui lui sont déclarés, le relevé des temps d'intervention des personnalités politiques dans les médias tenu par le Conseil supérieur de l'audiovisuel et les travaux de recherche[75]. Sans énoncer explicitement un droit à la portabilité, ces données doivent être mises à disposition dans un format ouvert, qui soit aisément réutilisable. Par exemple, en vertu de l'article 23 de la LRN, les données de consommation et de production d'électricité et de gaz doivent être mises « à disposition du public par voie électronique, dans un format ouvert, aisément réutilisable et exploitable par un système de traitement automatisé sous une forme agrégée garantissant leur caractère anonyme. ».

1.3. Wiederverwendungsrecht des Ergebnisses oder der anonymisierten Daten

Wie unter 1. erwähnt ist das Ergebnis der Datenverarbeitung nur Gegenstand des Herausforderungsrechts gemäss Art. L-224-42, soweit es sich um nicht persönliche Daten handelt und soweit die Datenverarbeitung nicht eine «wesentliche Bereicherung» darstellt. Was genau eine wesentliche Bereicherung darstellt, wird auf Verordnungsstufe festgelegt. Der

---

[73] Art. L. 224-42-3 Ziff. 1 und 2 : « Art. L. 224-42-3.-Sans préjudice des dispositions protégeant le secret en matière commerciale et industrielle et des droits de propriété intellectuelle, tout fournisseur d'un service de communication au public en ligne propose au consommateur une fonctionnalité gratuite permettant la récupération :
« 1° De tous les fichiers mis en ligne par le consommateur ;
« 2° De toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause. Ces données sont récupérées dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé ;

[74] Art. L. 224-42-3 Ziff. 3 : « 3° D'autres données associées au compte utilisateur du consommateur et répondant aux conditions suivantes :
« a) Ces données facilitent le changement de fournisseur de service ou permettent d'accéder à d'autres services ;
« b) L'identification des données prend en compte l'importance économique des services concernés, l'intensité de la concurrence entre les fournisseurs, l'utilité pour le consommateur, la fréquence et les enjeux financiers de l'usage de ces services.

[75] Cela est énoncé respectivement aux articles 3, 17, 18, 23, 55, 15 et 30 de la LRN, qui insèrent des dispositions dans divers codes, par exemple le code des relations entre le public et l'administration.

Dienstleistungserbringer muss beweisen, dass die Datenverarbeitung einer wesentliche Bereicherung gleichkommt. (Art. L. 224-42-3 Abs. 3).

2. Droits d'utilisation du contenu numérique

Il existe différents moyens en droit français d'autoriser et de limiter l'utilisation ou la réutilisation de données par un tiers, notamment un concurrent. Au niveau de l'autorisation, le contrat de licence est possible pour les logiciels ; et pour les données numériques en général, la notion de « contrat de fourniture de contenu numérique » a été insérée en droit français sous l'impulsion de l'Union européenne. En ce qui concerne la limitation du droit d'utilisation ou de réutilisation d'un contenu digital, c'est-à-dire de la protection de ce contenu et de son créateur, le droit de la propriété intellectuelle (particulièrement le droit d'auteur) est applicable en premier lieu, et le droit de la concurrence en second lieu.

2.1. Autorisation d'utilisation du contenu numérique

Tout d'abord, le droit français prévoit la possibilité de conclure un **contrat de licence** concernant les **logiciels** uniquement.[76]. Toutefois, selon la doctrine, ce type de contrat pourrait être étendu à tout contenu digital[77].

Pour les données numériques en général, la cession de celles-ci est possible par un **contrat de fourniture de contenu numérique**. Ce type de contrat est mentionné dans la loi n° 2014-344 du 17 mars 2014 relative à la consommation, dite loi « Hamon », qui transpose en droit français la **directive 2011/83/UE relative aux droits des consommateurs**[78]. Cette loi a inséré de nouvelles dispositions relatives aux contrats de fourniture de contenu numérique dans le Code de la consommation dans un chapitre Ier, Titre II, Livre II de la Partie législative nouvelle[79], concernant les règles de formation et d'exécution des contrats conclus à distance et hors établissement. L'article L. 221-4, alinéa 2 de ce code prévoit ainsi que les dispositions de ce chapitre « s'appliquent également aux contrats portant

---

76 Le contrat de licence d'utilisation, ou simplement licence, est une sorte de prêt du logiciel pour une durée déterminée, contrairement à une vente où le transfert de propriété est définitif. La différence entre la licence et la vente est cependant parfois difficile à cerner. Voir : J. Huet, CONTRATS INFORMATIQUES . – Contenu et typologie, in Encyclopédie du Jurisclasseur : Contrats-Distribution, LexisNexis, 20 Mars 2013, Fasc. 2415 ; Concrètement, le contrat de licence permet d'autoriser l'utilisation d'un logiciel, et de définir les limites de cette utilisation. Cette autorisation se fait en vertu de l'article L. 122-6 du Code de la propriété intellectuelle (CPI), et l'article L. 122-6-1 du même code donne davantage de précisions sur les actes soumis à autorisation ou non de l'auteur pour que le tiers bénéficie pleinement de son droit d'utilisation. Il conviendra alors, pour le créateur, de fixer les modalités d'utilisation du logiciel par un contrat de licence avec l'utilisateur. L'une des clauses importantes à faire figurer dans ce contrat concerne la propriété intellectuelle, à savoir l'étendue des droits qui sont concédés par l'auteur à l'utilisateur (H. Bitan, Droit des créations immatérielles : logiciels, bases de données, autres œuvres sur le Web 2.0, Rueil-Malmaison: Lamy, 2010, pp. 198-199). Il est également possible de conclure des licences dites « libres », c'est-à-dire que l'auteur autorise la copie, la modification et la diffusion, mais il ne transfère pas les droits d'auteur attachés au logiciel (J.-M. Bruguière & M. Vivant, Droit d'auteur et droits voisins,).

77 J.-M. Bruguière & M. Vivant, Droit d'auteur et droits voisins, éd. Dalloz, 3e édition, 2016, pp. 751-768.

78 Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, disponible sous : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A32011L0083 (13.12.2017)

79 Cette dénomination vient de la modification du Code de la consommation par l'Ordonnance n° 2016-301 du 14 mars 2016 relative à la partie législative du code de la consommation.

sur la fourniture de contenu numérique indépendamment de tout support matériel. ». Dans le Code de la consommation, le contenu numérique est défini comme « des données produites et fournies sous forme numérique »[80]. La notion de contrat de fourniture de contenu numérique n'est pas définie et reste floue. Les dispositions y relatives ne précisent pas la nature de ce contrat, s'il s'agit d'une vente ou d'une licence, mais exposent les particularités de ce type de contrat, en termes d'informations précontractuelles ou de droit de rétractation par exemple. Le contrat de fourniture de contenu numérique sans support matériel serait plus propice à la location, du fait de cette dématérialisation[81], et donc à une cession temporaire de données numériques (contrat de licence). Mais dans cette hypothèse, reste à préciser si cette fourniture ne consiste qu'en un droit d'accès, ou si le consommateur pourrait également réutiliser le contenu numérique en vertu d'un contrat de licence[82].

A noter enfin que le **droit de la propriété intellectuelle** permet à un créateur d'empêcher ou de limiter les utilisations non autorisées de son œuvre par des **mesures techniques de protection**[83]. Par exemple, il est possible de demander un mot de passe afin d'empêcher les copies illicites. Mais cette pratique est susceptible de limiter également les droits des utilisateurs autorisés, notamment par l'impossibilité de procéder à toute copie, illicite ou non. Parmi les mesures techniques de protection, les systèmes numériques de gestion des droits visent spécifiquement à autoriser ou interdire notamment l'utilisation d'une œuvre par le titulaire des droits[84]. Cependant, ces mesures de protection visent avant tout à limiter les utilisations non autorisées uniquement, et ne concernent que le cas où le contenu numérique est protégé par le droit d'auteur. De plus, les logiciels sont expressément exclus du champ d'application de l'article L. 331-5 du CPI, présentant ces mesures de protection.[85]

2.2. Protection du contenu numérique

Concernant la **protection d'un contenu digital et de son créateur**, il convient d'abord de préciser que celle-ci se fait en premier lieu par le **droit d'auteur**[86]. En effet, le CPI, dans la première partie relative à la propriété littéraire et artistique, en son article L. 112-1 prévoit que « Les dispositions du présent code protègent les droits des auteurs sur toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination. ». Un contenu digital peut être considéré comme une œuvre de l'esprit, sa forme de diffusion ou son support de communication n'en faisant pas une œuvre à part. Le créateur bénéficie du droit d'auteur si son œuvre est protégeable[87], et peut à ce titre autoriser ou refuser l'utilisation de celle-ci. Le tiers, notamment le concurrent, qui utiliserait ou réutiliserait un contenu numérique protégé par le droit d'auteur risquerait d'être sanctionné pour contrefaçon[88].

---

80 Art. L. 221-1 du Code de la consommation. Cette définition provient de la directive 2011/83/UE (article 2, pt 11), et le considérant 19 de celle-ci précise : « Par contenu numérique, on entend les données qui sont produites et fournies sous une forme numérique, comme les programmes informatiques, les applications, les jeux, la musique, les vidéos ou les textes, que l'accès à ces données ait lieu au moyen du téléchargement ou du streaming, depuis un support matériel ou par tout autre moyen. ».

81 J. Sénéchal, Le contrat de fourniture de contenu numérique en droit européen et français : une notion unitaire ou duale ?, Revue de l'Union européenne 2015, p. 442

82 M. Behar-Touchais et al., Fourniture, Contrats Concurrence-Consommation n°2, février 2017, dossier 5 ; pour le projet de Directive au niveau européen, cf. A..

83 Art. L. 331-5, al. 1 du CPI.

84 H. Bitan, Droit des créations immatérielles, *op. cit.*, pp. 233-234.

85 Pour plus d'informations sur ces mesures de protection, voir : A. Latreille, MESURES TECHNIQUES DE PROTECTION ET D'INFORMATION, in Encyclopédie du JurisClasseur : Propriété littéraire et artistique, LexisNexis, 19 Avril 2011 (dernière mise à jour : 16 Février 2015), Fasc. 1660.

86 H. Bitan, Droit des créations immatérielles, *op. cit.*, pp. 103-174.

87 La condition est qu'elle soit originale.

88 Une contrefaçon est un délit civil et pénal sanctionnant les atteintes aux œuvres de l'esprit protégées par le droit d'auteur. Ce délit aboutit à une procédure de saisie-contrefaçon.

Pour certains types de contenus digitaux, une **protection particulière** est mise en place. Tel est le cas de la protection s'appliquant aux **bases de données**. La spécificité de ces dernières est d'être constituées de données réunies dans un ensemble qui forme la base[89], et la protection par le droit d'auteur varie alors si l'on s'intéresse à la base de données ou seulement aux éléments individuels de la base. Ainsi, la base dans son ensemble est considérée comme une création de l'esprit dès lors qu'elle comporte une certaine mise en forme[90], et bénéficie alors de la protection classique apportée par les dispositions du droit d'auteur. La simple compilation de données n'est donc pas protégeable au titre du droit français, il est nécessaire qu'il y ait une structuration, un agencement original de la base.

Cependant, la protection de l'ensemble de la base de données ne s'étend pas aux éléments qui sont intégrés à celle-ci, c'est-à-dire aux données brutes contenues dans la base. Sans disposition applicable à ces données[91], ces dernières pourraient être réutilisées sans limite par un tiers. Afin de remédier à cela, une protection particulière est accordée au producteur de la base de données : un **droit sui generis.** Ce droit est régi aux articles L. 341-1 à L. 343-7 du CPI. La condition pour bénéficier de ce droit sui generis est un investissement financier, matériel ou humain substantiel de la part du producteur de la base de données pour l'élaboration de cette dernière[92]. Lorsque ce critère d'investissement substantiel est rempli, le producteur de la base bénéficie du droit sui generis et peut alors s'opposer à l'extraction et à la réutilisation de la totalité ou d'une partie substantielle des données de la base par un concurrent[93], voire à l'extraction et à la réutilisation répétées et systématiques de parties non substantielles du contenu de la base de données si cela constitue un usage anormal de la base de données[94]. Par exemple, dans une affaire impliquant l'Agence France-Presse (AFP), cette dernière a pu interdire la réutilisation des dépêches de sa base de données par une société concurrente car cette réutilisation d'une partie du contenu de la base excédait les conditions normales d'utilisation de la base de données[95]. Des **limites** à ce droit sui generis existent toutefois, notamment en vertu du **droit de la concurrence**. En effet, si les données de la base sont une ressource essentielle pour les opérateurs qui exercent une activité concurrentielle, le producteur ne peut pas monopoliser les informations de la base de données en imposant le paiement d'un prix excessif pour y avoir accès[96]. C'est par exemple le cas de la liste des abonnés au téléphone[97]. Lorsque les données contenues dans la base constituent une ressource essentielle, le droit sui generis ne peut être appliqué et les données peuvent être librement réutilisées par un concurrent.

De manière générale, le **droit de la concurrence** apporte une **protection complémentaire au droit d'auteur** pour le contenu digital. Ce sont les règles générales du droit de la concurrence qui s'appliqueront, il n'y a pas de règles spécifiques en matière de données numériques. Bien que la concurrence soit par principe libre, cela n'est pas sans limite et les entreprises ne peuvent user de procédés dits contraires aux usages loyaux du commerce[98]. Le créateur de contenu numérique pourra alors être protégé par l'action en concurrence déloyale ou en concurrence parasitaire dans le cas où un tiers aurait réutilisé le contenu digital sans autorisation. La première permet d'obtenir réparation à la suite d'un acte déloyal (dénigrement, imitation de produits …) de la part d'un concurrent qui a

---

89 La base de données est définie à l'art. L. 112-3 al. 2 du CPI.

90 Les critères étant le « choix et la disposition des matières » (art. L. 112-3 al. 1 du CPI).

91 Tel est le cas lorsque les données constituent en elles-mêmes des œuvres originales protégeables.

92 Art. L. 341-1 CPI.

93 Art. L. 342-1 CPI.

94 Art. L. 342-2 CPI.

95 T. Com. Paris, 5 février 2010, AFP c/ Topix Technologies et Topix Presse.

96 S. Jouve, Le Code de la propriété intellectuelle comme fondement de l'appropriation de l'information par l'entreprise de communication ?, Legicom, 2013, p. 18 ss.

97 Exemple tiré de Cass. Com., 23 mars 2010, 08-20.427 08-21.768, inédit.

98 Mémento Concurrence-Consommation, Editions Francis Lefebvre, 2017, p. 163 ss.

résulté en un préjudice. L'action en concurrence parasitaire vise quant à elle à sanctionner ceux qui profitent des fruits de l'effort économique d'autrui, qu'ils soient concurrents ou non. La concurrence déloyale et le parasitisme sont semblables[99] et sont tous deux sanctionnés sur le fondement de la responsabilité civile extracontractuelle (articles 1240 et 1241 du Code civil[100]). Sur la base de ces articles, il est nécessaire de démontrer une faute, un préjudice et un lien de causalité entre les deux. La faute est la pratique déloyale employée par le concurrent ou tiers non concurrent, par exemple l'imitation de produits d'un concurrent ou encore **la réutilisation d'un contenu digital sans autorisation**. Il faut ensuite un préjudice causé à la victime. Il s'agit généralement d'un préjudice matériel tel que la perte d'exploitation. Enfin, le demandeur devra prouver qu'il existe un lien de causalité entre la faute commise et le préjudice subi. L'action en concurrence déloyale ouvre droit à des dommages et intérêts. La victime d'agissements déloyaux peut aussi agir par voie de référé afin d'obtenir la cessation des pratiques en cause.[101]

Le droit de la concurrence peut donc s'appliquer en cas de réutilisation non autorisée de données par un concurrent. Toutefois, les **actions en concurrence déloyale et en parasitisme** d'une part, et l'**action en contrefaçon** d'autre part ne peuvent être invoquées pour les mêmes faits[102]. C'est une protection alternative au droit d'auteur. Ainsi, le droit de la concurrence, et particulièrement les actions en concurrence déloyale ou parasitisme, peut protéger l'organisme qui crée un contenu numérique dans la mesure où le contenu n'est pas protégé par le droit de la propriété intellectuelle, ou si les **faits** invoqués pour ces actions sont **distincts** de ceux de l'action en contrefaçon qui sanctionne une atteinte au droit d'auteur. Si le contenu numérique n'est pas éligible à la protection par le droit d'auteur, par exemple si l'œuvre n'est pas originale, alors le créateur peut demander réparation sur la base des articles 1240 et 1241 du Code civil dans le cas où un concurrent (ou tiers non concurrent) aurait réutilisé ce contenu sans autorisation et aurait donc commis un acte déloyal[103]. Cela est plus compliqué si les données sont protégées par le droit de la propriété intellectuelle. Dans ce cas, la victime des agissements déloyaux devra invoquer des faits distincts de ceux de l'action en contrefaçon, même si celle-ci a été rejetée, afin d'obtenir réparation au titre de l'action en concurrence déloyale ou parasitisme. De même pour les bases de données, une action en concurrence déloyale et parasitisme pourra être faite cumulativement à une condamnation sur le fondement du droit sui generis si on est en présence de faits distincts. Pour terminer, il faut noter toutefois que l'action en contrefaçon peut aller jusqu'à la condamnation pénale du fautif, alors que les actions en concurrence déloyale et parasitaire n'ouvrent droit qu'à des dommages et intérêts.

---

99 Il existe toutefois quelques nuances entre les deux notions, voir : P. le Tourneau, PARASITISME . – Notion de parasitisme, in Encyclopédie du JurisClasseur : Concurrence - Consommation, LexisNexis, 2017, Fasc. 570.

100 Anciennement les articles 1382 et 1383 du Code civil, modifiés par l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations .

101 Sur les actions en concurrence déloyale et parasitaire : Mémento Concurrence-Consommation, *op. cit.*

102 H. Bitan, Droit des créations immatérielles, *op. cit.*, pp. 178-179 ; et Mémento Concurrence-Consommation, *op. cit.*.

103 La Cour d'appel de Paris l'a par exemple rappelé pour l'action en parasitisme dans un arrêt du 5 avril 1990 où il est énoncé que « si le droit de propriété des intimées n'avait pas été établi, elles auraient été fondées, par référence aux articles 1382 et 1383 du Code civil [devenus articles 1240 et 1241], à demander réparation d'agissements parasitaires ayant permis de s'approprier à moindres frais les fruits de l'effort économique d'autrui et quand bien même aucune situation concurrentielle n'aurait existé entre les parties », CA Paris, 4e ch., 5 avril 1990.

3. Devoir de donner accès à l'Etat

3.1. Devoir de donner accès à l'Etat en général

En France, des dispositions spécifiques sont prévues concernant les **traitements de données personnelles pour le compte de l'Etat** dans la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après LIFL)[104]. Cette loi, en vigueur dès 1978, énonce les règles en matière de protection des données personnelles, et a été modifiée par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique qui introduit en droit français certaines dispositions du règlement général de l'Union européenne sur la protection des données[105].

En vertu des principes énoncés dans la LILF, les traitements de données personnelles par l'Etat sont autorisés par arrêté ministériel[106]. La particularité des traitements effectués pour le compte de l'Etat est que ce dernier peut accéder aux données personnelles et les utiliser, voire les réutiliser, à des fins spécifiques **sans le consentement de la personne concernée**. Ce principe est énoncé à l'article 32, V. de la LIFL qui énonce :

> « I.-La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant :
> 1° De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
> 2° De la finalité poursuivie par le traitement auquel les données sont destinées ;
> 3° Du caractère obligatoire ou facultatif des réponses ;
> 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
> 5° Des destinataires ou catégories de destinataires des données ;
> 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort ;
> 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne ;
> 8° De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée. […]
> V. Les dispositions du I ne s'appliquent pas aux données recueillies dans les conditions prévues au III et utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et **intéressant la sûreté de l'Etat, la défense, la sécurité publique** ou ayant pour **objet l'exécution de condamnations pénales ou de mesures de sûreté**, dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement. »

La LIFL prévoit également qu'« il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. ». Cette interdiction comporte toutefois des dérogations, notamment pour l'accès et la réutilisation de données par l'Etat.[107]

---

104 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible sous : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&dateTexte=20171211 (13.12.2017)

105 Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

106 Article 26 de la LIFL.

107 Cf. *infra*, points 3.2. et 3.3. sur les traitements de données personnelles à des fins de santé publique et statistiques.

L'accès et la réutilisation de données par l'administration publique dans des domaines spécifiques sont également réglementés par les dispositions de différents codes ou lois. Nous nous intéresserons ici particulièrement aux domaines de la santé publique et des statistiques.

3.2. Accès à des données dans le domaine de la santé

Dans le domaine de la **santé publique**, les dispositions relatives à la mise à disposition des données de santé, et à leur éventuelle réutilisation, se trouvent dans le Code de la santé publique (ci-après CSP)[108]. L'article L. 1460-1 du CSP présente tout d'abord les principes généraux relatifs à la mise à disposition et aux traitements de données de santé en disposant :

> « Les données de santé à caractère personnel recueillies à titre obligatoire et destinées aux services ou aux établissements publics de l'Etat ou des collectivités territoriales ou aux organismes de sécurité sociale peuvent faire l'objet de traitements à des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public, dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les traitements réalisés à cette fin ne peuvent avoir ni pour objet ni pour effet de porter atteinte à la vie privée des personnes concernées. Sauf disposition législative contraire, ils ne doivent en aucun cas avoir pour fin l'identification directe ou indirecte de ces personnes.
> Les citoyens, les usagers du système de santé, les professionnels de santé, les établissements de santé et leurs organisations représentatives ainsi que les organismes participant au financement de la couverture contre le risque maladie ou réalisant des recherches, des études ou des évaluations à des fins de santé publique, les services de l'Etat, les institutions publiques compétentes en matière de santé et les organismes de presse ont accès aux données mentionnées au premier alinéa dans les conditions définies par la loi n° 78-17 du 6 janvier 1978 précitée et, le cas échéant, par les dispositions propres à ces traitements. »

Il est donc prévu d'une part un **accès aux données de santé à caractère personnel** notamment aux services de l'Etat et institutions publiques compétentes en matière de santé[109], et d'autre part, la possibilité, en particulier pour les services ou établissements publics de l'Etat, de **traiter ces données à des fins de recherche, d'étude ou d'évaluation** qui présente un intérêt public[110]. Il est précisé que ces traitements doivent respecter la LIFL, notamment les principes énoncés aux articles 32 et 8 de la LIFL présentés ci-dessus[111]. L'utilisation des données de santé par l'Etat doit également respecter la vie privée des personnes concernées, et ne doit pas permettre l'identification de celles-ci.

L'accès aux données de santé, et leur utilisation par l'Etat, peut aussi se faire par le biais du **système national des données de santé** (SNDS)[112]. Le SNDS est alimenté notamment par les organismes d'assurance maladie, les établissements de santé et l'Institut national de la santé et de la recherche médicale, en regroupant leurs bases de données incluant différentes catégories de données de santé[113], particulièrement les informations relatives aux bénéficiaires de soins et prestations médico-sociales, aux organismes d'assurance maladie, à la prise en charge des bénéficiaires, et les informations concernant les professionnels et services de santé[114]. Deux types d'accès aux données du SNDS sont prévus : un **accès permanent** pour certains services publics ou organismes publics pour

---

108 Particulièrement dans les parties législative et réglementaire du CSP, sous le titre VI intitulé « Mise à disposition des données de santé » du livre IV de la première partie. Ce titre VI a été introduit par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

109 Art. L. 1460-1 du CSP al. 2.

110 Art. L. 1460-1 du CSP al. 1.

112 Les dispositions y relatives sont les articles L. 1461-1 à L. 1461-7 (partie législative) du CSP, et articles R. 1461-1 à R. 1461-19 (partie réglementaire) du CSP.

113 CNIL, SNDS : Système National des Données de Santé, 18 avril 2017, disponible sous : https://www.cnil.fr/fr/snds-systeme-national-des-donnees-de-sante (12.12.2017)

114 Art. R. 1461-4, I du CSP.

l'**accomplissement de leurs missions**, et un **accès ponctuel** soumis à autorisation de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour les autres organismes (privés notamment) ou les organismes publics hors du cadre fixé, aux **fins de recherche, d'étude et d'évaluation**[115]. En vertu de l'article R. 1461-11 du CSP, « I.-Les services de l'Etat, les établissements publics et les organismes chargés d'une mission de service public, mentionnés à l'article R. 1461-12, sont autorisés à traiter des données à caractère personnel du système national des données de santé, dans des limites définies aux articles R. 1461-13 et R. 1461-14, en fonction des exigences des missions de service public qu'ils remplissent. […] ». Les établissements et organismes publics énoncés à l'article R. 1461-12[116] bénéficient donc d'un accès permanent aux données de santé pour les traitements nécessaires à l'accomplissement de leurs missions[117].. Concernant l'accès ponctuel à des fins de recherche, d'étude ou d'évaluation, la réutilisation des données du SNDS doit se faire dans un but de recherche répondant à un motif d'intérêt public et contribuer à l'une des finalités énoncées au III de l'article L. 1461-1 du CSP, c'est-à-dire : « 1° A l'information sur la santé ainsi que sur l'offre de soins, la prise en charge médico-sociale et leur qualité ; 2° A la définition, à la mise en œuvre et à l'évaluation des politiques de santé et de protection sociale ; 3° A la connaissance des dépenses de santé, des dépenses d'assurance maladie et des dépenses médico-sociales ; 4° A l'information des professionnels, des structures et des établissements de santé ou médico-sociaux sur leur activité ; 5° A la surveillance, à la veille et à la sécurité sanitaires ; 6° A la recherche, aux études, à l'évaluation et à l'innovation dans les domaines de la santé et de la prise en charge médico-sociale. » .

En plus de l'alimentation du SNDS, l'article L. 6113-8, al. 1 du CSP dispose que « Les établissements de santé transmettent aux agences régionales de santé, à l'Etat ou à la personne publique qu'il désigne et aux organismes d'assurance maladie les informations relatives à leurs moyens de fonctionnement, à leur activité, à leurs données sanitaires, démographiques et sociales qui sont nécessaires à l'élaboration et à la révision du projet régional de santé, à la détermination de leurs ressources, à l'évaluation de la qualité des soins, à la veille et la vigilance sanitaires, ainsi qu'au contrôle de leur activité de soins et de leur facturation. ». Les **établissements de santé**, publics ou privés, sont donc tenus de transmettre notamment les informations relatives à leurs données sanitaires à l'Etat, aux agences régionales de santé ou aux organismes d'assurance maladie aux fins prévues par cet article L. 6113-8. En vertu de l'article L. 3113-1 du CSP, les **professionnels de santé** ont l'obligation de transmettre les données individuelles concernant certaines maladies à l'autorité sanitaire, dans un but de conduite et d'évaluation de la politique de santé publique. Ils doivent aussi communiquer les données de santé aux organismes d'assurance maladie obligatoire conformément à l'article L. 161-29 du code de la sécurité sociale[118], la base de données de ces organismes étant ensuite incluse dans le SNDS.

Il faut également noter que les **données personnelles de santé** sont considérées comme des données sensibles et bénéficient à ce titre d'une **protection particulière** qui encadre la collecte et le traitement de celles-ci. L'article 8 de la LIFL dispose ainsi qu'il « est interdit de collecter ou de traiter des données à caractère personnel […] relatives à la santé » des personnes. Toutefois, des **dérogations** sont possibles pour :

---

115 Art. L. 1461-3, I du CSP.

116 Il s'agit par exemple de la direction générale de la santé, des agences régionales de santé, des caisses de l'assurance maladie, de l'Agence nationale de santé publique et de l'Institut national des données de santé.

117 Cela est réglementé par les articles R. 1461-11 à R. 1461-19 du CSP.

118 Sur les obligations de communication des données des professionnels de santé : CNIL, Communiquer des données de santé, 11 juin 2009, disponible sous : https://www.cnil.fr/fr/communiquer-des-donnees-de-sante-0 (13.12.2017)

> « 1° Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée ;
> 2° Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
> 3° Les traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical : - pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme ; - sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité ; - et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
> 4° Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée;
> 5° Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
> 6° Les traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du code pénal ;
> 7° Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels dans le respect de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, après avis du Conseil national de l'information statistique et dans les conditions prévues à l'article 25 de la présente loi ; 8° Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé selon les modalités prévues au chapitre IX. »[119].

Les traitements des données de santé à caractère personnel effectués pour le compte de l'Etat sont permis, soit afin d'assurer la sûreté de l'Etat, la défense ou la sécurité publique, soit pour prévenir, rechercher, constater ou poursuivre des infractions pénales, ou exécuter des condamnations pénales[120]. Dans ce cas, l'Etat peut utiliser ou réutiliser les données personnelles relatives à la santé d'une personne aux fins précédemment énoncées, lorsque le traitement a été autorisé par arrêté ministériel après avis motivé de la CNIL. Il est également possible pour les organismes ou services chargés d'une mission de service public de traiter les données de santé en cas d'alerte sanitaire[121]. La réutilisation des données à des fins de recherche, d'étude et d'évaluation est également envisagée par la LIFL au chapitre IX concernant les « Traitements de données à caractère personnel à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé ».

3.3 Accès à des données à des fins statistiques

En matière de **statistiques**, l'accès aux données et la réutilisation de celles-ci est possible. La loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques[122] prévoit une **obligation pour les personnes morales de droit privé** de transmettre les données qu'elles détiennent pour les besoins d'enquêtes statistiques obligatoires menées par les services de statistiques publique, c'est-à-dire l'Institut national de la statistique et des études économiques (INSEE) et les services

119 Article 8, II. de la LIFL.

120 Art. 26, I et II, de la LIFL.

121 Art. 22, V de la LIFL.

122 Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques, disponible sous : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000888573&categorieLien=cid (13.12.2017)

statistiques ministériels[123] (et la **cession des données** relatives aux personnes physiques et aux personnes morales, recueillies par une administration ou une personne morale de droit public ou privé qui gère un service public, à l'INSEE ou aux services statistiques ministériels[124]). Cette obligation découle d'une décision du ministre de l'économie. Une telle obligation n'est pas prévue pour les personnes physiques mais celles-ci ont toutefois un devoir de répondre avec exactitude et dans les temps à ces enquêtes[125]. Les données cédées peuvent ensuite être réutilisées par l'INSEE ou les services statistiques ministériels à des fins de statistiques uniquement[126]. La **réutilisation des données à caractère personnel relatives à la santé** est limitée aux fins d'établissement de statistiques sur l'état de santé de la population, les politiques de santé publique ou les dispositifs de prise en charge par les systèmes de santé et de protection sociale en lien avec la morbidité des populations[127].

La loi relative à l'informatique, aux fichiers et aux libertés précédemment citée a également introduit certaines dispositions sur la **collecte et les traitements de données à des fins statistiques**, qui dérogent aux principes généraux relatifs aux traitements de données. Concernant spécifiquement les **statistiques publiques**, l'INSEE et les services statistiques ministériels ne sont pas soumis à l'interdiction de collecter et de traiter certaines données personnelles, à savoir celles « qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci »[128]. En outre, le traitement de données à des fins historiques, statistiques ou scientifiques déroge aux principes de conservation des données personnelles[129] et à la nécessité de finalités déterminées, légitimes et explicites de la collecte de celles-ci[130]. En effet, le responsable du traitement doit normalement collecter les données personnelles pour des finalités déterminées et en informer la personne concernée, mais la réutilisation à des fins statistiques notamment n'est pas soumise à ce principe. Toutefois, cette réutilisation doit se faire dans le respect des principes et procédures de la LIFL[131] et les données ne peuvent être utilisées pour prendre des décisions à l'égard des personnes concernées[132].

---

123 Art. 3 bis, I de la loi n° 51-711, introduit par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique : « I. - Le ministre chargé de l'économie peut décider, après avis du Conseil national de l'information statistique, que les personnes morales de droit privé sollicitées pour des enquêtes transmettent par voie électronique sécurisée au service statistique public, à des fins exclusives d'établissement de statistiques, les informations présentes dans les bases de données qu'elles détiennent, lorsque ces informations sont recherchées pour les besoins d'enquêtes statistiques qui sont rendues obligatoires en application de l'article 1er bis. ».

124 Art. 7 bis, al. 1 de la loi n° 51-711.

125 Art. 3 de la même loi.

126 L'art. 7 bis, al. 1 de la même loi dispose « à des fins exclusives d'établissement de statistiques ».

127 Art. 7 bis, al. 2 à 6 sur les traitements de données de santé à des fins statistiques.

128 Art. 8, I (interdiction) et II, 7° (exception pour les statistiques publiques) de la LIFL.

129 Art. 32, III, et 36, al. 1 de la LIFL.

130 Art. 6, 2° et 32, III de la LIFL.

131 Il s'agit des conditions de licéité des traitements (art. 6 et 7 de la LIFL), l'accomplissement des formalités préalables (chapitre IV de la LIFL) et l'obligation d'information préalable pour responsables de traitements (section 1 du chapitre V de la LIFL).

132 A. Debet et al., Informatique et libertés – La protection des données à caractère personnel en droit français et européen, Lextenso éditions, 2015, pp. 336-337.

D. SCHWEDEN

1. Datenportabilität

Die aktuelle Datenschutzgesetzgebung enthält soweit ersichtlich kein Recht auf Datenportabilität. Die entsprechende Regelung in der DSGVO wird als Neuheit beschrieben. Es finden sich soweit ersichtlich auch keine Bestimmungen zur Wiederverwendung des Ergebnisses der Datenverarbeitung oder anonymisierter Daten.

2. Gewähren von Nutzungsrechten an digitalen Inhalten

In Sweden, the **main legal protection for databases/digital content is provided in the Act on Copyright in Literary and Artistic Works** (Copyright Act) (*Lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk*). In accordance with its Chapter 5 section 49, a database is protected either if a large number of information items have been compiled (catalogue protection) or if it is the result of a significant investment (sui generis right). This will be discussed in section 2.1.

Certain complementary protection of databases is provided through the **rules on unfair competition in the Marketing Practices Act** (*Marknadsföringslag (2008:486)*. They will be examined in section 2.2.

There are no specific rules applicable specifically to the **licencing of databases/digital content**, instead the general principles and rules on commercial transaction in the Sale of Goods Act (*Köplag (1990:931)*) apply by analogy (section 2.3).

2.1 The Catalogue Protection and Sui Generis Right in the Copyright Act

The protection of databases was first introduced in the beginning of the 1960th through the adoption of the so-called **catalogue protection** (*katalogskyddet)* in Chapter 5 section 49 in the Copyright Act aiming to protect catalogues, tables and other similar works where a large amount of data was collected and gathered. It was introduced as a right closely related to an intellectual property right in order to protect collections not sufficiently creative to enjoy copyright protection.[133] The object of protection was works such as timetables and telephone catalogues. The catalogue protection was however not aimed at protecting the information as such, but rather the work needed for the collection and gathering.[134] About the same time, a similar catalogue protection provision was laid down in the Copyright Acts of other Nordic countries. The sui generis right in the EU Database Directive[135] is partly bases on this "Nordic catalogue protection".[136]

In 1997, **the catalogue rule was amended in order to implement the Database Directive** that, in addition to protection for the structure, lays down a sui generis right for the *content* of databases. The current Chapter 5 section 49 first paragraph in the Copyright Act reads as follows:

> *Anyone who makes a catalogue, a table or similar work in which a large quantity of data has been collected or which is the result of substantial investment has an exclusive right to produce copies of the work and provide public access to it.*

---

133 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 87.

134 Government bill Prop. 1960:17, p. 269.

135 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

136 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 87.

Accordingly, the provision **protects a database for (1) the compilation of a large number of information items (catalogue rule) or (2) if it is the result of a significant investment (*sui generis right*).**

The first possibility of protection under Chapter 5 section 49 in the Copyright Act (a **large number of information item**s compiled) applies typically to sales and exhibition catalogues, timetables, compilations of currency and stock exchange prices.[137] In a judgment from 1985, the Supreme Court found that a collection of cards containing information about plants was a work protected under the catalogue rule.[138] The collection included information about 64 plants and the number of the total information/data was about 1250. In its finding that that constituted *a large number of information*, the Court referred to the fact that the compilation of the information required a significant amount of time.

The second possibility of protection under Chapter 5 section 49 in the Copyright Act **(the result of significant investment – sui generis right) transposes Article 7 of the Database Directive** into Swedish law. It may however be noted that Chapter 5 section 49 in the Copyright Act does not refer to the different phases in the processing work - obtaining, verification or presentation of the contents – that according to the Directive are subject to protection. Neither are there any references to the fact that the investment can be substantial both qualitatively and quantitatively. However, the Supreme Court has found that the provision sufficently meets these requirements in the Directive.[139]

The producer of the database, who can be either a legal or a natural person, has an "**exclusive right to produce copies of the work and provide public access to it**".[140] As a point of departure, this exclusive right is similar to that applicable to actual copyright. In that aspect, the Swedish law lays down a **wider and to some extent different protection** than provided for in Article 7.1 of the Database Directive.[141]

The database does not have to reach a certain **quality or originality** in order to enjoy protection. Where a certain level of originality is reached it can however be protected as a literary work according to Chapter 1 section 2 in the **Copyright Act**. For the purposes of this report, we will however not discuss collection of data protected as literary work.

The **term of protection for databases is 15 years** from the year of its completion. In the case the database is made available to the public, the term of protection expires 15 years from the year when it was first made available to the public. This is in accordance with the term of protection laid down in Article 10 in the Database Directive.[142]

2.2 Unfair Competition under the Marketing Practices Act

Since the 1970ies, the protection against unfair competition in Swedish law has been anchored in rules on marketing (commercialisation). Therefore, the regulatory framework on unfair competition has as a point of departure been concerned with how different measures taken by companies affect the consumers as a whole rather than departing from tort law principles with respect to pecuniary

137 C. Kirchberger et al., Cyber Law in Sweden, 2nd ed., Wolters Kluwer, 2014, p. 112.

138 Högsta Domstolens dom i mål nr T93-85 (NJA 1985 s. 813).

139 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 264 commenting case NJA 2005 s. 924.

140 Copyright Act Chapter 5 section 49, para. 1.

141 A. Olin, Lexino –djupa lagkommentarer till Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk, Karnov 2017, commentary to Chapter 5 section 49.

142 Copyright Act Chapter 5 section 49, para. 2.

damages (including unjust enrichment). This is probably an important reason to the **absence in Swedish law of a general protection against unfair competition** by slavish imitation and free-riding (*snyltning)* in relation to the investments or other measures taken (object protection).[143]

The need to introduce a general clause against "traditional" unfair competition has been discussed in the doctrine.[144] However, in the context of implementing the requirement in the EU Directive on Unfair Commercial Practices[145] the lawmaker held that there was no need to adopt such general clause.[146]

A victim of unfair competition therefore needs to **rely on the protection offered under the Marketing Act, which essentially is limited to matters involving marketing** (*marknadsföring)*.[147] In the context of the protection of unauthorised use of digital content examined in this part of the study, the relevant rule in the Marketing Act is the general clause on so-called generally excepted marketing practices expressed in section 5 and 6 in the Act. The prohibition on imitation embedded in the general clause focuses on a requirement of confusion (*förväxling)*. However, as protection was considered necessary also in situations where there are no risk of confusion, a complementary prohibition against free-riding (*renommésnyltning)* without the element of confusion has been developed in case law. This prohibition hinders the "free rider" to use the commercial value that involves the consumer's positive perception built up by and attributed to the other party. [148] Given that the **protection requires an assessment from the perspective of the recipient of the marketing**, it protects only the results of the investments and not the investments as such.[149]

2.3 Licensing

So-called licensing contracts (*licensavtal*) are used when an intellectual property right holder grants a right to someone to use the protected material. While a "licensavtal" can be considered as a specific kind of contract type, it is essentially unregulated.[150] Accordingly, there are no specific legal provisions governing licensing contracts of intellectual property protected databases/digital content.[151] In the absence of any specific legislation, it is widely accepted that the general rules on commercial transaction in the Sale of Goods Act (*Köplag (1990:931)*) apply analogously to the extent that the

---

143 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 71.

144 Ibid, p. 53.

145 DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council.

146 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 53.

147 Marketing Practices Act (*Marknadsföringslag (2008:486)),* section 1.

148 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 50 and cases there referred to. In a case decided in 2006 (MD 206:13) concerning the newspaper and website Metro, the Market Court examined the limits on the protection against unfair competition concerning databases. One question concerned the provision of Metro's website and its functions. Metro offered a service that enabled the user to access ads on other companies' websites. The user was re-directed to the ad and informed that such re-direction was made. The Court found that such a measure was not violating the general clause in the Marketing Act.

149 J. Axhamn, Databasskydd, Stocholm: Stockholm University, 2017, p. 51.

150 U. Bernitz et al., Immaterialrätt och otillbörlig konkurrens, 13th ed., Stockholm: Jure 2013, p. 414.

151 The same is true for contracts concerning the use of databases/digital content that do not involve intellectual property rights but that are protected under the catalogue rule or the sui generis right (see section 2.1).

contracts does not stipulate otherwise.[152] The parties therefore have considerable autonomy (freedom of contract) when agreeing on their licencing contracts.[153] Licensing contract are generally in writing although it is not a formal requirement. Where no time limitation is agreed, the contract is normally considered to have an indefinite duration. However, either parties have the right to terminate such "indefinite duration contract" while respecting a reasonable notice period that apply generally to long term contracts.[154]

As regards *software licencing contracts*, it may however be mentioned that the Copyright Act (Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk) contains certain rules setting out specific provisions with regard to both the transfer of copyright to software as well as licensing.[155] Given that these rules are specific for *software* licencing and not include licencing of databases/digital content other than software, they will not be subject to further examination.

3. Verpflichtung zur Gewährung des Zugangs an den Staat

Public authorities can oblige an individual or a juridical person to give access to data that they possess only where this is explicitly provided for in law. Such obligation can be imposed in different areas and for different purposes. This report will however focus on the legal framework in the area of public health (3.1.) and statistics (3.2.). Given that such obligation is an important tool in law enforcement (i.e. for the prevention of crimes) we will also examine the key rules in that area (3.3). These are the Code of Judicial Procedure's rules on seizure and the rules obliging electronic communication service providers to disclose certain information under the Electronic Communications Act and the Act on Retrieval of Data on Electronic Communication by Law Enforcement Agencies.

3.1 Obligation to Share Data for Public Health Purposes

The system of rules obliging individuals and judicial person to share data with the public administration is complex. This report will not examine the system exhaustively but aims to give a comprehensive overview and an examination of its key features and rules.

For a better understanding, it may be useful to start by briefly describing the organisation of health care in Sweden. The responsibility for health and medical care in Sweden is shared by the central government, county councils (*landsting)* and municipalities (*kommuner)*. The role of the central government is to establish principles and guidelines, and to set the political agenda. The tools for this are the adoption of laws and ordinances or by reaching agreements with the Swedish Association of Local Authorities and Regions (*Sveriges Kommuner och Landsting - SKL*), which represents the county councils and municipalities. Although there are a number of private organisation providing health care, the regional and local **public agencies are the major health care providers**.

The Health and Medical Service Act (*Hälso- och sjukvårdslag (1982:763*)) regulates the responsibilities of county councils and municipalities, and gives local governments a certain margin of discretion within the health care. The Act lays down the basic principle that every council must offer good health and medical care but may outsource certain parts of the care.[156]

---

152 C. Kirchberger et al., Cyber Law in Sweden, 2nd ed., Wolters Kluwer, 2014, p. 131.

153 U. Bernitz et al., Immaterialrätt och otillbörlig konkurrens, 13th ed., Stockholm: Jure 2013, p. 414.

154 Ibid.

155 Ibid, p. 132.

156 The Health and Medical Service Act (*Hälso- och sjukvårdslag (1982:763)*) Chapter 7 section 3.

There are a number of laws regulating the obligations of health care providers. A key piece of legislation is the Patient Safety Act (*Patientsäkerhetslag (2010:659)*) that regulates the basic requirements for health care providers, their registration, and supervision.

The **Patient Data Act (*Patientdatalag (2008:355)*) regulates processing of personal health data** within health and medical services. This means that it regulates health care records and it applies in addition to the general rules in the Swedish Personal Data Act (*Personuppgiftslag (1998:204)*). The Patient Data Act contains both rules on so-called electronic health care records (*elektroniska patientjournal)* and regular health care records.[157] All health providers are obliged to have a system for keeping patient journals and the creation of a health care record is therefore not dependent on the patient's consent.[158] However, a patient has the right to opt-out to systems of direct access to the records between different health care providers.[159] Such systems of direct access (*sammanhållen journalföring)* have been implemented in all county councils and enable the health care professional to access their patient's entire health care record.[160] Basic rules on the disclosure of health care records and certain information duties are laid down in Chapter 5 of the Patient Data Act. These are rather technical but essentially state that disclosure of information concerning a patient is only possible upon the patient's permission.

Important limitations to disclose information are also laid down in the **Public Access to Information and Secrecy Act ("the Secrecy Act") (*Offentlighets- och sekretesslagen (2009:400)*) and the Patient Safety Act**.[161] The key provisions concern rules on secrecy for health care professionals. The Secrecy Act applies to public health care providers and the Patient Safety Act applies to private health care providers. Although some of the rules are formulated differently, these laws essentially provide the same level of integrity protection and secrecy obligations.[162]

Chapter 25 in the Secrecy Act regulates secrecy within health care. The main rule provides that information about an individual's health or other personal information is **subject to secrecy unless it is obvious that disclosure would not in any way harm the person concerned** or anyone closely related to him or her.[163] The fact that an information is subject to secrecy means essentially that the information cannot be disclosed. However, there are exceptions to this basic rule. The more important rules allowing for exception will be examined in the following.

According to Chapter 5 section 11 in the Secrecy Act, a public body (*myndighet)* that provide health care may **disclose an information to another public body** providing health care if they belong to the same county council or municipality. This exception allows for county councils and municipalities to

---

157 For a description of the Swedish electronic health records system see for example C. Kirchberger, Overview of the national laws on electronic health records in the EU Member States – National Report for Sweden, 2014, available at https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_sweden_en.pdf (11.12.2017).

158 Patient Data Act (Patientdatalag (2008:355)) Chapter 3 section 1.

159 Ibid, Chapter 6 section 2.

160 Ibid, Chapter 6, information about the direct access available for example at https://www.1177.se/Vastra-Gotaland/Regler-och-rattigheter/Sammanhallen-journalforing/ (13.12.2017).

161 Ibid, Chapter 5 section 1 and 2.

162 Government bill Prop 1993/94:149 Åligganden för personal inom hälso- och sjukvården m.m. p. 120.

163 Secrecy Act (*Offentlighets- och sekretesslagen (2009:400)*) Chapter 25 section 1.

freely choose how to organise their health care without taking into account that secrecy in principle applies between public authorities.[164]

Secrecy does not apply to information shared between public authorities if the **information is crucial in order for the individual to receive necessary treatment**. This applies for example in cases of serious drug abuse and in case of pregnancy if it is necessary in order to take measures to protect the baby.[165]

An information duty applicable to both public and private provision of health care is laid down in the Patient Safety Act. According to this duty, **health care professionals must disclose the following information** (including information subject to secrecy):

- Information whether a person has been treated at a health care institution if that information is requested in an individual case by a court, the prosecutor, the Police authorities, the Enforcement Authority (*Kronofogdemyndigheten)* and the Tax Agency (*Skatteverket)*;
- information needed for pursuing the activity of personal protection of members of parliament, the government and the royal family if that information is requested by the Swedish Security Service (*Säkerhetspolisen)*;
- information needed for forensic analysis;
- information requested by the the National Board of Health and Welfare's (*Socialstyrelsen*) Legal Advisory Board on certain legal, social and medical issues determines certain specific cases in order to pursue its activities.
- information needed to decide a case concerning dismissal of a student from university education or from the police academy.
- Information needed to decide on a person's suitability to have a driving licence or to be a licenced taxi driver.[166]

The **Social Services Act (*Socialtjänstlag (2001:453)*)** concerning the protection of children and youth contain certain provisions obliging individuals and entities working with children to report to the local social welfare board (*socialnämnden)* any knowledge or suspicion that a child is being mistreated.

There is a general duty upon health care providers to provide the supervisory authority - the Health and Social Care Inspectorate (*Inspektionen för vård och omsorg)* – with any information needed for its supervision.[167]

An information duty is also laid down in Chapter 2 section 5 in the Communicable Diseases Act (*Smittskyddslag (2004:168)* according to which a **health care professional must report certain so called public danger diseases** (*allmänfarliga sjukdomar)* to the county council's doctor in charge of such diseases and to the Public Health Agency (*Folkhälsomyndigheten)*.[168] This applies to both public and private health care professionals.

Finally, according to the **Act on Health Care Data Register** (*Lag (1998:543) om hälsodataregister)* and a number of Government Ordinances, health care providers have a duty to submit various information (including personal data) to a number of registers held by certian designated central government

---

164 L. Lundgren, Commentary to Offentlighets- och sekretesslagen (2009:400), Commentary to Chapter 25 section 11 no 436, Karnov Juridik online database, 2017.

165 Secrecy Act (*Offentlighets- och sekretesslagen (2009:400)*) Chapter 25 section 12.

166 Patient Safety Act (*Patientsäkerhetslag (2010:659)*) Chapter 6 section 15.

167 Patient Safety Act (*Patientsäkerhetslag (2010:659)*) Chapter 7 section 20.

168 A definition of public danger diseases is laid down in the Communicable Diseases Act (*Smittskyddslag (2004:168)* Chapter 1 section 3. Complementary and more detailed rules on the reporting requirement are laid down in a Government Ordinance on Communicable Diseases (*Smittskyddsförordning (2004:255))*.

agencies: the National Board of Health and Welfare's (*Socialstyrelsen*), the Medical Products Agency (*Läkemedelsverket)* and the the Public Health Agency (*Folkhälsomyndigheten)*. Personal data in those register may only be used for (1) statistical purposes; (2) follow-up, evaluation and quality assurance of the health care; and (3) research and epidemiological studies.[169]

It may also be mention that there exist so-called **national and regional quality registers** (*nationella och regionala kvalitetsregister)*. These registers contain a variety of patient-related data gathered from several caregivers about diagnoses, measures taken, results of treatment, etc. The aim is to measure and develop the quality of health care services.[170] An individual must be consulted before his or her personal data is processed in the register and have the right to oppose to such processing.[171] There are currently 96 national quality registers.[172]

3.2 Obligation to Share Data for Official Statistical Purposes

Statistics Sweden (Statistiska cetralbyrån – SCB) is the main public authority in Sweden responsible for official statistics. It is tasked with the development, production and dissemination of statistics and to coordinate the system for the official statistics. In addition to SCB, the government has appointed 27 government agencies to be responsible for official statistics within their respective areas. These are listed in the Government Ordinance on the Official Statistics (*Förordningen (2001:100) om den officiella statistiken*) and include among others the National Board of Health and Welfare's (*Socialstyrelsen*) and the Social Insurance Agency (*Försäkringskassan)*.[173]

Rules on obligation to share data for official statistical purposes are laid down in the **Official Statistics Act (*Lag (2001:99) om den officiella statistiken*)** and in the above mentioned Government Ordinance on the Official Statistics. This obligation concern primarily individuals or any type of organization pursuing an economic activity, as well as municipalities and county councils.[174] There is wide range of information that must be submitted including the name and identification number for the person pursuing an economic activity, the number of employees, prices for goods and services, energy consumption, etc.[175] The designated government agencies that are responsible for official statistics can also oblige any other government agency to submit the information needed in order to produce official statistics.[176]

So-called **sensitive personal data can only be processed to the extent it is explicitly permitted** in the annex to the Government Ordinance on the Official Statistics.[177] Statistics on crimes may for example

---

169 Act on Health Care Data Register (*Lag (1998:543) om hälsodataregister)* section 3. Information on hälsodataregister is available at http://www.socialstyrelsen.se/register/halsodataregister (13.12.2017).

170 Patient Data Act (Patientdatalag (2008:355)) Chapter 7 section 1.

171 Patient Data Act (Patientdatalag (2008:355)) Chapter 7 section 2. Information on national and regional quality register is available at http://kvalitetsregister.se/tjanster/omnationellakvalitetsregister.1990.html (13.12.2017).

172 http://kvalitetsregister.se/tjanster/omnationellakvalitetsregister.1990.html (13.12.2017).

173 Government Ordinance on the Official Statistics (*Förordningen (2001:100) om den officiella statistiken* Bilaga.

174 Official Statistics Act (*Lag (2001:99) om den officiella statistiken*) section 7.

175 See Government Ordinance on the Official Statistics (*Förordningen (2001:100) om den officiella statistiken* sections 5 to 5d and 6.

176 Government Ordinance on the Official Statistics (*Förordningen (2001:100) om den officiella statistiken* section 6.

177 Government Ordinance on the Official Statistics (*Förordningen (2001:100) om den officiella statistiken* section 8.

only contain sensitive personal data that concern criminal acts, court decisions and coercive measures. Personal data used for statistic purposes that can be traced to an individual is subject to secrecy.[178]

In case of failure to submit the requested information, the authority requesting the information can order the submission subject to a fine.[179]

3.3 Access to Data for Law Enforcement Purposes

2.1.1.1. 3.3.1 General rules on seizure in the Code of Judicial Procedure

Seizure (*beslag)* is a criminal procedure measure of coercion through which law enforcement authorities, investigating a suspected crime, may confiscate (seize) objects that could be relevant to the investigation, and later serve as evidence. General applicable rules on seizure (*beslag)* are laid down in Chapter 27 in the Code of Judicial Procedure (*Rättegångsbalk (1942:740)*).

According to Chapter 27 Section 1 in the Code of Judicial Procedure, seizure may include objects that could reasonably be expected to have significance for the investigation of a crime or that could be the product of criminal activity. A seizure does not require the identification of a suspect and can be carried out following any type of crime and be directed at any person or entity. The general rules on seizure **apply to devices containing electronically stored data**, for example on a computer or a mobile phone.[180]

2.1.1.2. 3.3.2 Electronic Communications

Electronic messages and telecommunication not contained in a physical object cannot be seized under the general rules on seizure in the Code of Judicial Procedure. However, law enforcement authorities may access such information in accordance with provisions laid down in other laws.

An important law in this regard is the **Electronic Communications Act (*Lag (2003:389) om elektronisk kommunikation*)** which contains rules obliging providers of a publicly available electronic communications service to provide certain information to law enforcement authorities. Thus, providers may be obliged to grant access for the police to information and identification of an individual.[181] Information about *the content* of an electronic message can however only be ordered by a court and for offences with a punishment of minimum two years imprisonment.[182]

Finally, it may also be mentioned that the **Act on Retrieval of Data on Electronic Communication by Law Enforcement Agencies** (*Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*) allows the police and customs to request traffic data, including location data, under certain circumstances with regards to their intelligence activities. Any such request has to be reported to a specific supervisory authority, the Swedish Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden*).[183]

---

178 Secrecy Act (*Offentlighets- och sekretesslagen (2009:400)*) Chapter 24 section 8.

179 Official Statistics Act (*Lag (2001:99) om den officiella statistiken*) section 20.

180 See case NJA 2015 s. 631.

181 Electronic Communications Act (*Lag (2003:389) om elektronisk kommunikation*) Chapter 6 section22.

182 P. Andersson, Commentary to (Lag (2003:389) om elektronisk kommunikation), Commentary to Chapter 6 section 22 no 311, Karnov Juridik online database, 2017.

183 C. Kirchberger, Cyber Law in Sweden, Wolters Kluwer, 2014, p. 232.

E. JAPAN

1. Datenportabilität

Das japanische Datenschutzrecht wurde 2016 revidiert und die revidierte Gesetzgebung ist am 30. Mai 2017 in Kraft getreten. Das neue Recht führt insbesondere Pflichten für die Bearbeitung anonymisierter Daten ein (Kapitel 4 Absatz 2 des Gesetzes). Der betroffenen Person werden aber weder für die persönlichen noch für die anonymisierten Daten Rechte auf die Herausgabe zur Nutzung / Weiterverwendung eingeräumt.[184]

Im Rahmen einer im Sommer 2017 publizierten Untersuchung einer Studiengruppe «Data and Competition Policy» der Wettbewerbskommission[185] wurde allerdings hervorgehoben, dass **mittelfristig Massnahmen nötig** sein würden, um der Dominanz gewisser Social Networking Seiten zu begegnen. Aktuell scheinen aber die Widerstände in der Wirtschaft gegenüber der Einführung eines Rechts auf Datenportabilität zu gross.[186]

Im November 2017 haben das Ministerium für Handel und Wirtschaft (*Ministry of Economy, Trade and Industry)* und das Innen- und Kommunikationsministerium (*Ministry of Internal Affairs and Communications*) eine **Arbeitsgruppe zur Datenportabilität** eingesetzt.[187] Demnach sollen Herausforderungen und Auswirkungen der Einführungen eines Rechts auf Datenportabilität untersucht werden und die Problematik aus der Perspektive der Konsumenten und der Wirtschaft allgemein sowie in verschiedenen Sektoren wie Gesundheit, Finanzdienstleistungen, Energie untersucht werden.[188] Resultate liegen soweit ersichtlich noch nicht vor.[189]

Zu erwähnen ist, dass die japanische Datenschutzgesetzgebung lediglich Auskunfts- und Löschungsrechte der betroffenen Person über die Bearbeitung von persönlichen Daten vorsieht (Art. 28 PIPA).

2. Gewähren von Nutzungsrechten an digitalen Inhalten

Die japanische **Datenschutzgesetzgebung** sieht für persönliche Daten lediglich ein Widerspruchsrecht gegen die Bearbeitung unrechtmässig erworbener Daten vor (Art. 30 PIPA) sowie gewisse Schutzmechanismen (gegenüber dem Rückgängigmachen der Anonymisierung) bei der Bearbeitung

---

184 Dies bestätigt im Report of Study Group on Data and Competition Policy, Japan Fair Trade Commission / Competition Policy Research Center, 06.06.2017, verfügbar unter http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.files/170606-4.pdf (06.09.2017), S. 17.

185 Englische Pressemitteilung vom 06.06.2017 verfügbar unter http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.html, Zusammenfassung verfügbar unter http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.files/170606-3.pdf

186 T. Sekiguchi, Big Data, antimonopoly law study may put brakes on Japan's data market growth, 07.06.2017, verfügbar unter https://mlexmarketinsight.com/insights-center/editors-picks/Data-Protection-Privacy-and-Security/asia/big-data,-antimonopoly-law-study-may-put-brakes-on-japans-data-market-growth (05.09.2017).

187 Pressemitteilung des Ministry of Economy, Trade and Industry vom 20.11.2017, verfügbar unter http://www.meti.go.jp/english/press/2017/1120_002.html sowie diejenige des Innen- und Kommunikationsministeriums (mit leicht abweichendem Inhalt), verfügbar unter http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/171120_03.html.

188 S. die beiden zitierten Pressemitteilungen; s. auch .

189 Auskunft der Korrespondentin Wakako Oshima vom 10.04.2018.

von anonymisierten Daten. Das japanische **Urheberrecht** schützt Daten allgemein ebenfalls nicht. Das Urheberrechtsgesetz (Copyright Act) enthält aber Bestimmungen zum Schutz von «**Zusammenstellungen**» (*Compilations*, Art. 12[190]) sowie **Datenbanken** (Art. 12bis)[191]. Erstere sind dann wie ein «Werk» geschützt, wenn sie aufgrund der Auswahl oder Zusammenstellung der Inhalte eine «intellektuelle» Schaffung sind. Bei zweiten hängt der Schutz davon ab, ob die **Auswahl** oder der **systematische Aufbau** der Information eine «intellektuelle Schaffung» ausmacht. Entsprechend können Datenbanken oder Zusammenstellungen – gleich wie andere geschützte Werke - Gegenstand von Nutzungsrechten gemäss dem Urheberrechtsgesetz sein.[192]

Die Rechtsprechung hat in mehreren Urteilen darüber befunden, wann eine Datenbank urheberrechtlich geschützt wird und wann nicht. So wurde in einem jüngeren Urteil auf die Auswahl und die Struktur und systematische Zusammenstellung abgestellt, um eine «Beziehungsdatenbank» zu schützen.[193] Aus der Rechtsprechung geht ebenfalls hervor, dass auch die Kopie von einer Datenbank, welche nicht urheberrechtlich geschützt ist, zu **Schadenersatzansprüchen** berechtigen kann, wenn für die Zusammenstellung viel Zeit und ein grosser Aufwand erforderlich war.[194] Der Aufwand zur Erstellung einer Datenbank rechtfertigt somit allein keinen urheberrechtlichen Schutz, kann aber durchaus (bei einer «ungerechten und nicht zu rechtfertigen Ausnutzung der Leistung»[195]) Ansprüche begründen. So erstaunt nicht, dass anscheinend über die Verwendung von Daten durchaus vertragliche Vereinbarungen getroffen werden.[196] Soweit ersichtlich wird auch für Übertragung von Nutzungsrechten an Daten (mindestens in der englischen Übersetzung) der Begriff «Lizenz» verwendet.[197]

Die Übertragung bzw. vor allem die Weigerung zur Übertragung von Daten an Konkurrenten kann schliesslich **wettbewerbsrechtlich relevant** sein.[198]

---

190 "**Article 12.** (1) Compilations (not falling within the term "databases"; the same shall apply hereinafter) which, by reason of the selection or arrangement of their contents, constitute intellectual creations shall be protected as independent works.
(2) The provisions of the preceding paragraph shall not prejudice the rights of authors of works which form part of compilations defined in that paragraph.", Übersetzung gemäss Y. OYAMA et al., Copyright Law of Japan, Copyright Research and Information Law Center.

191 "**Article 12*bis*.** (1) Databases which, by reason of the selection or systematic construction of information contained therein, constitute intellectual creations shall be protected as independent works.
(2) The provisions of the preceding paragraph shall not prejudice the rights of authors of works which form part of databases defined in that paragraph." Übersetzung gemäss Y. Oyama et al., Copyright Law of Japan, Copyright Research and Information Law Center

192 Art. 63 ff. Copyright Act.

193 Intellectual Property High Court, 19.01.2016, Urteil zusammengefasst von W. Oshyma.

194 Tokyo District Court, 28.03.2002, Urteil zusammengefasst von W. Oshyma.

195 So gemäss Tokyo District Court, 28.03.2002, Urteil zusammengefasst von W. Oshyma.

196 So gemäss Auskunft per E-Mail vom 13.01.2018 von W. Oshyma.

197 So im Report of Study Group on Data and Competition Policy, Japan Fair Trade Commission / Competition Policy Research Center, 06.06.2017, verfügbar unter http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.files/170606-4.pdf (06.09.2017), S. 51 und 57 f.

198 Report of Study Group on Data and Competition Policy, Japan Fair Trade Commission / Competition Policy Research Center, 06.06.2017, verfügbar unter http://www.jftc.go.jp/en/pressreleases/yearly-2017/June/170606.files/170606-4.pdf (06.09.2017), S. 42 ff. und S. 51 ff.

3. Verpflichtung zur Gewährung des Zugangs an den Staat

Soweit ersichtlich besteht in Japan keine allgemeine Pflicht von Privatpersonen, dem Staat Zugang zu Daten bzw. Auskunft zu erteilen. Entsprechende Pflichten scheinen aber in verschiedenen Gesetzen vorgesehen. So sieht das **Statistikgesetz** (*Statistics Act*[199]) eine Auskunftspflicht von natürlichen und juristischen Personen vor (Art. 13), aber auch ein Recht der Behörde, welche eine genehmigte «Grundstatistik» (*fundamental statistical survey*) durchführt, zu Räumlichkeiten Zugang zu erhalten und das Vorlegen von Information («material») zu verlangen (Art. 15). Daten sind nicht ausdrücklich genannt, könnten aber möglicherweise darunter fallen. Eine damit verbundene Pflicht zum Vorlegen von Information und Material ist in Art. 108-3 Abs. 3 des Industrie- und Arbeitsgesundheitsgesetzes (*Industrial Safety and Health Law*[200]) vorgesehen. Sie richtet sich an Arbeitgeber, Arbeitnehmer und «betroffene Personen», welche dem Gesundheits-, Arbeits- und Wohlfahrtsministerium Auskunft bzw. Zugang im Rahmen von Erhebungen zur Ermittlung der Zusammenhänge zwischen chemischen Substanzen am Arbeitsplatz oder anderer Verhältnisse und der Gesundheit (Epidemiological Survey) geben müssen. Es erscheint wahrscheinlich, dass ähnliche Pflichten auch in anderen Gesetzen bestehen.

Im **Gesundheitsbereich** sieht das Gesetz über Infektionskrankheiten (*Act on the Prevention of Infectious Diseases and Medical Care for Patients with Infectious Diseases*)[201] Meldepflichten der Ärzte und Tierärzte (sowie Tierbesitzer) für den Fall vor, dass gewisse Krankheiten diagnostiziert werden (Art. 12 und 13). Von gewissen Grippepatienten (*Novel Influenza*) kann die Auskunft über gemessene Temperatur und andere Gesundheitsinformationen verlangt werden (Art. 44-3). Eine allgemeine Auskunfts- oder Zugangspflicht ist soweit ersichtlich im betreffenden Gesetz nicht vorgesehen.

F. USA

1. Datenportabilität

In den USA führte das *Office of Science and Technology Policy*, welches der Exekutive angegliedert ist, im September 2016 eine Konsultation zur Einführung der Datenportabilität durch.[202] Weder das Ergebnis der Konsultation noch weitere Massnahmen diesbezüglich sind aktuell ersichtlich.

Inwieweit entsprechende Rechte durch Rechtsprechung, in spezifischen Gesetzen oder/und auf Ebene der Gliedstaaten bestehen, konnte im Rahmen der aktuellen Untersuchung nicht ermittelt werden.

---

199 Act No. 53 of May 23, 2007, in englischer Sprache verfügbar unter https://unstats.un.org/unsd/vitalstatkb/KnowledgebaseArticle50572.aspx sowie unter http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=02&dn=1&co=01&ia=03&x=0&y=0&ky=statistics&page=25

200 Law No 57 vom 08.06.1972, zuletzt geändert durch GLaw No. 25 vom 31.05.2006, verfügbar in englischer Sprache unter https://www.jniosh.go.jp/icpro/jicosh-old/english/law/IndustrialSafetyHealth_Law/11.htm.

201 Act 114 1998, geändert durch Act 115 2014.

202 A. Macgillivray & J. Shjambaugh, Exploring Data Portability, verfügbar unter obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability (01.09.2017).

2. Verpflichtung zur Gewährung des Zugangs an den Staat

2.2. General Issues

2.2.1. Introduction

The historical roots of the United States as a nation that separated from a colonial power whose officers regularly intruded upon the homes, businesses, and persons of its citizens has been read into the Constitution as well as infused into its approach to defining the permissible relationship between the government and the people. The aversion to unlimited governmental intrusion does not make demands for property – or information – impossible, but it makes such demands presumptively illegitimate. The government requires, therefore, the approval of a court or other judicial officer ("magistrate") to require an individual to give up information and the right of the individual to refuse such demands is protected in a number of Constitutional provisions. While there is a significant difference in judicial approaches to the proper state-individual relationship in matters of criminal law, where defendant rights may be seen as undercutting societal interests of security, the basic principles of individual independence and limited government still heavily inform the jurisprudence.

2.2.2. Constitutional Aspects

The interaction of the government and an individual's data has been an arena of much discussion in the United States. There are a number of important Constitutional aspects of governmental demands for access to data – the Fourth Amendment is the main focus of the literature on data hand-over requests, but the Fifth Amendment is also relevant. There are a number of pieces of legislation that are also of relevance to the general obligation of persons to yield data to the State, including the All Writ's Act and the Communication Assistance to Law Enforcement Act (CALEA).

For holders of health data, the basic rules regarding compliance with governmental demands remain: the federal laws permitting courts to order a person to turn over data are still subject to Constitutional limitations. There are, however, a number of sector-specific frameworks in place to protect the heightened privacy interests contained by health data. These place particular demands on the data controller. The health data related laws are found on both the federal and State level. State laws vary widely as regards their specific content.

2.2.2.1. US Constitutional Prohibition on Unreasonable Search and Seizure by Government

Part of the so-called "Bill of Rights" added to the U.S. Constitution by the drafters of the original text, the Fourth Amendment protects a person's right to not be the target of the government's unreasonable search and seizure of their "persons, houses, papers, and effects".[203] The Fourth Amendment's protection against governmental intrusions does not give individuals a general "right of privacy", but the Supreme Court has interpreted the scope of its protections as extending to areas or possessions in which the individual has a subjective belief that they/it is private and that society would find this expectation of privacy to be reasonable.[204]

Scope

As the Court stated in Katz, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *[…]* But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[205] Thus, not only a person's

[203] U.S. Constitution, 4th Amendment.

[204] Katz v. United States, 389 U.S. 347, 361 (1967) (concurring opinion by Justice Harlan).

[205] Katz at 351.

"home", but also a telephone booth[206], a hotel room[207], or even luggage at an airport[208] may be protected spaces into which the government may not intrude absent a court order or other extenuating circumstance. Commercial buildings, too, are protected by the Fourth Amendment. The Court has noted that the "businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property". [209]

Warrant requirement

In order to search in these areas of expected privacy, the government agents must make an application to a court for a search warrant. The application must set forth the reasons for the search, describing with particularity what the agents expect to seize. If the court or magistrate determines that the agents have "probable cause", (s)he will grant the warrant, describing what can be searched and/or seized. Presented with a valid search warrant, a person must yield to the agents' search and seizure. Resistance would be contrary to a court order, and therefore punishable.

The warrant requirement of the Fourth Amendment extends to administrative actions as well as criminal ones.[210] The case of *Camara v. Municipal Court*[211] involved a man who refused to permit the housing inspector to enter his house for routine inspection without a warrant. In that case, the Supreme Court reaffirmed the Fourth Amendment's reasonableness requirement, but noted that the balance of interests are valid for administrative searches as well as for criminal searches. Thus, although there is clearly a public interest in building inspections, "the question is not whether the public interest justifies the type of search in question, but whether the authority to search should be evidenced by a warrant".[212] Given the relatively light burden of obtaining a search warrant, the Court found the privacy interest outweighed any public interest in conducting a warrantless search.

Warrant requirement exceptions

However, the warrant requirement for searches is not absolute. First, a person may consent to a search. The question of who may consent to a search of property shared by more than one person has been settled to permit a co-occupant's consent to be valid for at least the common areas or commonly used property.[213] A hotel owner, however, may not consent to the search of a customer's room under ordinary circumstances.[214]

---

[206] Katz v. United States, 389 U.S. 347 (1967).

[207] Stoner v. California, 376 U.S. 483 (1964). But see Jason C. Miller, Do Not Disturb: Fourth Amendment Expectations of Privacy in Hotel Rooms, 7:2 Seton Hall Circuit Rev. 269 (2010) (available at https://ssrn.com/abstract=1718669; viewed 9 December 2017).

[208] Torres v. Puerto Rico, 442 U.S. 465 (1979).

[209] Marshall v. Barlow's Inc., 436 U.S. 307, 311 (1978); See v. Seattle, 387 U.S. 541, 543 (1976).

[210] Marshall v. Barlow's Inc., 436 U.S. 307, 312 (1978). Note, however, that there are recognized exceptions to the warrant requirement for searches of alcohol and firearms companies, as these are "pervasively regulated". Id. at 313 (citing U.S. v. Biswell, 406 U.S. 311, 316 (1972) (firearms) and Colonnade Catering Corp. v. U.S., 397 U.S. 72, 72 (1970)). Consequently the Court considers that anyone who enters such a business knows of the extensive governmental interference and can be presumed to have assumed, or consented to, "the burdens … of their trade". Marshall v. Barlow at 313.

[211] Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523 (1967).

[212] Camara v. Municipal Court, 387 U.S. at 533.

[213] United States v. Matlock, 415 U.S. 164 (1974); Frazier v. Cupp, 394 U.S. 731 (1969). If, however, one co-owner consents and the other refuses, consent does not exist. Georgia v. Randolph, 547 U.S. 103 (2006).

[214] Stoner v. California, 376 U.S. 483 (1964).

Second, the Constitution only prohibits "unreasonable" searches[215] – and in some contexts, a warrantless search is reasonable if the government had cause to believe they would find evidence of a legal violation. A "stop and frisk" action, for example, may be carried out on a person if an officer has a reasonable suspicion – a lower standard than "probably cause" - that a crime has been committed.[216] Third, the warrant is only necessary for searches or seizures of objects/in places in which a person has an expectation of privacy. Thus, if evidence is in "plain view" from a place in which the officer was legally, it may be seized. The Court based the so-called "automobile exception" to the search warrant requirement, set forth in the 1925 case of Carroll v. US[217] (and developed over a long line of cases since then), on its determination that the mobility of the automobile means that the police do not have to get a warrant to search it for contraband. A warrantless search of an automobile is thus legal as long as the government authorities have probable cause to believe that the car contains evidence of a criminal act.[218]

A similar reduction of the privacy a person can expect can arise if the person has given a third party access to the information. In United States v. Miller, the Supreme Court set forth an "assumption of risk" view of the Fourth Amendment to delineate whether a "search" had even taken place. The Miller Court noted,

> "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[219]

This line of reasoning continued with the Supreme Court's 1979 *Smith v. Maryland* decision.[220] "When he used his phone," the Court wrote, "petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed".[221]

Finally, a warrant exception exists for "exigent circumstances", which include threats to the agent's safety or the danger that evidence will get destroyed within the time it takes to get a warrant. This exception balances the government's interests in performing the search with the individual's privacy rights.

The balancing, or reasonableness, test has expanded from exigent circumstances in recent years. According to some, it has opened the door to a trend of balancing these threats with the individual's privacy interest, something that can only be harmful for a protection of privacy.[222]

---

[215] This is the position adopted by the Supreme Court, but not the only possible interpretation of the text. See Esther Jeanette Windmueller, Reasonable Articulable Suspicion - The Demise of Terry v. Ohio and Individualized Suspicion, 25:3 Univ. Richmond L. Rev. 543, 545-546, (1991).

[216] Terry v. Ohio, 392 U.S. 1 (1968).

[217] Carroll v. United States, 267 U.S. 132 (1925).

[218] Id.

[219] United States v. Miller, 425 U.S. 435, 443 (1976)

[220] 442 U.S. 735 (1979).

[221] Id. at 744.

[222] See Fourth Amendment — Search and Seizure —Searching Cell Phones Incident to Arrest — Riley v. California, 128 Harv. L. Rev. 251, 257 (2014):

> "In case after case, the Roberts Court has liquidated bright-line rules about when a search is unreasonable and welcomed the "ascendance of 'reasonableness balancing' as a dominant mode of constitutional inquiry."

(citing Erin Murphy, The Supreme Court, 2012 Term — Comment: License, Registration, Cheek Swab: DNA Testing and the Divided Court, 127 Harv. L. Rev. 161, 183 (2013) (available at http://harvardlawreview.org/wp-content/uploads/2014/10/riley_v_california.pdf; visited 6 December 2017).

Consequences of an illegal search

The Constitutional principle known as the "exclusionary rule" prevents any evidence gleaned from an illegal search or seizure to be used in a criminal proceeding against the victim of the action. An extension of the exclusionary rule also prohibits the use at trial of evidence obtained by means of other illegally obtained evidence. A person who believes a search or seizure to have been in violation of the warrant requirement and to not fall within one of the recognized exceptions may therefore challenge any charges on this basis.

Importantly, however, the Supreme Court found the exclusionary rule to extend only to criminal prosecutions. While an administrative search may require a warrant, a warrantless search in such a case will not result in the evidence being excluded from evidence. This rule is based on a balancing test which places a significant weight on governmental interests in regulation.[223]

With the rapid increase in the number of people using mobile telephones as a means of communication, questions of the extent to which a phone may be searched brought out further refinements of the settled line of case-law. These cases determined a number of things. First, a person has a reasonable expectation of privacy in her mobile telephone. Thus, for police to look through the contents of a telephone, there must be a valid warrant authorizing the search. Even following a person's arrest, a time in which the person has a reduced expectation of privacy, the police need to get a warrant to search the arrestee's telephone.[224] However, the Miller v. United States and Smith v. Maryland holdings may also apply to smart phone users' data held by their digital providers – that is, if the information they consensually give their internet provider is requested (or even demanded) by the government from that provider and legally secured, the individuals themselves will have no standing to bring a claim under the Fourth Amendment.

2.2.2.2. US Constitutional Prohibition on Compelled Self-Incrimination and Uncompensated Expropriations

Like the Fourth Amendment, the Fifth Amendment is a part of the Bill of Rights of the U.S. Constitution. The Fifth Amendment provides a number of protections to individuals, with two of potential interest to the question of governmental requests for data. First is the phrase "[n]o person shall be compelled in any criminal case to be a witness against himself" and second "nor shall private property be taken for public use, without just compensation".

Self-incrimination

The jurisprudence of the Supreme Court has set forth numerous underlying values justifying the Fifth Amendment's prohibition on forced self-incrimination, including the wish to avoid placing defendants in a position of either perjuring themselves or admitting guilt - a wish that is meant to underscore that it is the government's obligation to prove the guilt of an alleged criminal – and the desire to avoid abusive interrogation contexts.[225]

Importantly, the prohibition on compelled self-incrimination extends only to natural persons, not to companies or organizations.[226]

---

[223] See Immigration and Naturalization Service v. Lopez-Mendoza, et al., 468 U.S. 1032 (1994).

[224] Riley v. California, 571 U.S. –; 134 S. Ct. 2473 (2014)

[225] See American Bar Association, The Purpose and Scope of the Fifth Amendment Right Against Compulsory Self-Incrimination 3-5 (text available at http://apps.americanbar.org/abastore/products/books/abstracts/5090120chap1_abs.pdf, viewed 6 December 2017).

[226] Hale v. Henkel, 201 U.S. 43 (1906).

Compulsion

The Fifth Amendment protection on self-incrimination applies only to compelled testimonial statements or actions which are incriminating.[227] That is, it can be invoked to refuse to give answers in response to questions posed while in governmental "custody" or ones demanded by subpoena (including those accompanied by a writ from a court), either of which are considered "compelled".[228]

Incrimination

Incriminating statements are those in which the information or its production could be used in a current prosecution or in which the information that could lead to a prosecution and be used as evidence in the future. (While a person in a civil trial may refuse to answer questions, the fact of such refusal may be considered as an inference of guilt/liability by the decisionmaker.)

Testimonial

Finally, testimonial statements are any production of the mind. Acts can be testimonial, too, if they are "communicative".[229] Testimonial acts are, as the Court has stated, "when the act entails implicit statements of fact, such as admitting that evidence exists, is authentic, or is within a suspect's control."[230]

While the actual contents of files found on a computer are not considered testimonial themselves, the yielding of computer passwords and encryption codes are testimonial if the police have no other proof of the defendant's ownership of or control over the device.[231] The reasoning behind this is that "[p]roduction itself acknowledges that the document exists, that it is in the possession or control of the producer, and that it is authentic".[232]

Note, however, that a recent lower court case denied an accused the right to refuse to use his fingerprint to unlock his electronic device.[233] The court distinguishing the fingerprint from a password, finding nothing "testimonial" about biometrics. This can be seen as being in accordance with Supreme Court precedent which holds that fingerprints and blood samples, for example, are not testimonial.[234]

Limitations on the Right to Remain Silent

Recent Supreme Court case-law has narrowed the protections available under the Fifth Amendment and has stressed that the Fifth Amendment exists not to protect any expanded notions of privacy (as the prior Murphy v. United States[235] had implied), but rather as a "conditional protection of testimonial privacy subject to basic limits recognized before the framing and refined through immunity doctrine"[236]

Finally, a person cannot complain of a violation of Fifth Amendment rights by third party revelations. The Supreme Court has stated clearly that "a party incriminated by evidence produced by a third party sustains no violation of his own Fifth Amendment rights". Thus, a corporation receiving a subpoena for

---

[227] Fisher v. United States, 425 U.S. 391, 408-409 (1976).

[228] See Fisher v. United States, 425 U.S. at 408.

[229] See United States v. Doe, 465 U.S. 605, 612 (1984).

[230] Doe v. United States, 487 U.S. 201, 209 (1988).

[231] E.g., United States v. Fricosu, 841 F.Supp.2d 1232 (D. Col *2012*).

[232] United States v. Hubbell, 530 U.S. 27, 36 (2000).

[233] Commonwealth of Virginia v. David Charles Baust, Va. Cir. CR14-1439 (28 October 2014).

[234] Doe v. United States, 487 U.S. at 210.

[235] Murphy v. Waterfront Comm'n of N. Y. Harbor, 378 U.S. 52 (1964).

[236] United States v. Aloyzas Balsys, 524 U.S. 666, 692-693 (1998).

information may not refuse to comply with it on the grounds that such information would incriminate a client, even if the client may have expected the information to be treated with confidentiality.[237]

Compensation for Expropriation

Besides the protection against compelled self-incrimination, the Fifth Amendment stipulates that the government must compensate any owner of property whose property it expropriates. The relevance of this provision to the current case is that if the state would demand information of a person or a company and that information is considered "property" and has a commercial value, the government must pay the person the fair market value upon its taking.

The corollary to the compensation requirement is that the person has no right to refuse to yield the property. In case of disagreement, a complaint can be made only on the basis of the amount of compensation.

2.2.2.3. Third Party Obligation to Afford the State Access to Data

The third-party individual's obligation to afford governmental access to data is a related, but separate topic. It, too, however, is the object of vigorous legal debate in the United States. Not necessarily new, the issue received heightened attention in the 2016 (aborted) legal action between the Federal Bureau of Investigation and Apple Computers. In that case, US used its authority under the All Writs Act[238], a federal law from 1789 intended to give courts the authority to demand third persons to act so as to ensure the effectiveness of the judiciary. In the 2016 case, a federal court used its authority under the All Writs Act to demand that Apple Computer create a method by which it could decrypt the contents of an iPhone which the police had seized following a shooting incident in St. Bernadino. Suspecting information about the perpetrator of the shooting and his possible connections, the police had unsuccessfully attempted to unlock the phone to search its contents. With only ten attempts before the device would erase all data stored on it, the police requested and received a court order demanding that Apple – a private company – develop a "backdoor" for that phone.

When Apple refused to comply, a legal action started on the question of whether the government could compel a third party to create such a mechanism for permitting government access to personal data. The case settled, leaving the legal questions open.

2.3. Rules for Governmental Access to Personal Health Data

There are, as stated at the beginning of this country section, numerous pieces of legislation governing privacy of data, both on the national level and on the State level. Here there will only be mention made of the **most comprehensive acts** regarding governmental access to data and the major legislation regulating health data. Again, these laws are specific to data access, but Constitutional protections remain for affected individuals to challenge governmental demands or violations of privacy by means of obtaining data without the consent of the data subject.

A **growing concern with governmental access to health data** has emerged along with general concerns about governmental access to all types of data following Edward Snowden's revelations of the scope of clandestine efforts by the government to collect data in the name of national security. As set forth by the American Civil Liberties Union (ACLU), many healthcare facilities in the United States now inform their patients of the possibility that data will be yielded to the government by use of signs with text such as the following:

---

[237] *California Bankers Assn. v. Shultz,* 416 U.S. at 55 (citing *Johnson v. United States,* 228 U. S. 457, 228 U. S. 458 (1913); *Couch v. United States,* 40 U.S. at 40 U. S. 328").

[238] 28 U.S.C. §1651

"[…]We may disclose your health information to law enforcement officials for the following reasons:

- *To comply with court orders or laws that we are required to follow;*
- *To assist law enforcement officers with identifying or locating a suspect, fugitive, witness, or missing person;*
- *If you have been the victim of a crime and we determine that: (1) we have been unable to obtain your agreement because of an emergency or your incapacity; (2) law enforcement officials need this information immediately to carry out their law enforcement duties; and (3) in our professional judgment disclosure to these officers is in your best interest;*
- *If we suspect that your death resulted from criminal conduct;*
- *If necessary to report a crime that occurred on our property; or*
- *If necessary to report a crime discovered during an offsite medical emergency (for example, by emergency medical technicians at the scene of a crime)."*[239]

2.3.1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[240] was passed in order to make it easier for families and individuals to change health insurance providers without losing coverage. The Act is administered by the Department of Health and Human Services.

The Administrative Simplification Rules (Title II, HIPAA)

Because the HIPAA's aims necessitate the transfer of health information between providers, it also establishes particular rules applying to health providers (companies as well as individuals) to protect the privacy of the disclosed health data. Those provisions are contained in Title II of the HIPAA, called the Administrative Simplification provisions of the HIPAA (Title II). The 2013 Final Omnibus Rule updated certain provisions of the Title II rules to deepen the privacy protections on "identifiable health data"[241], including expanding the scope of the privacy requirements to include not only the covered

---

[239] ACLU, FAQ on Government Access to Medical Records, at footnote (i) (quoting from a "Notice of Privacy Practices 8 (2003)" at the Terence Cardinal Cook Health Care Center)(available at https://www.aclu.org/other/faq-government-access-medical-records#_edn1; accessed 9 December 2017).

[240] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191. See also HIPAA Administrative Simplification 45 CFR Parts 160, 162, and 164 (as amended through 26 March 2013).

[241] The protections are only for data that is "individually identifiable", meaning that data that can be linked to a specific individual:

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

provider, but also its "business associates" as well as extending the protection to fifty years after death of the data subject.[242] Note, however, that non-identifiable health data is not covered. Thus, conglomerated information, including statistics, is not subject to the HIPAA privacy rules.

Two pertinent definitions contained in the Act are those of "health service provider" and "disclosure":

> "*Covered entity* means:
>
> (1) A health plan.
>
> (2) A health care clearinghouse.
>
> (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
>
> *Disclosure* means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information."[243]

Significantly, the definition of "health plan" excludes public providers which have a "principal purpose" of providing direct healthcare to individuals.[244]

There are certain requirements on the covered healthcare entities (including their business associates) to afford governmental access to the health data they maintain. This is in the context of **compliance investigations**. As 42 USC 1301, Section 221 instructs the Secretary of HHS to establish a "Health Care Fraud and Abuse Data Collection Program", the Act includes powers for the HHS to certify compliance. This relies on having access to datasets. Thus, 45 CFR §164.502 states,

> *"(d) Access to Reported Information.—*
>
> *(1) Availability.--The information in the database maintained under this section shall be available to Federal and State government agencies and health plans pursuant to procedures that the Secretary shall provide by regulation."*

Disclosure Rules for judicial or administrative purposes

In §164.512, the follows a long section setting forth permissible disclosures of health information to governmental agents (as well as to third parties).[245] The general standard is set out at §164.512(a):

> *"(a) Standard: Uses and disclosures required by law. (1) A covered entity may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law."*[246]

There is a separate provision for disclosures of health information for **public health purposes**.[247] Twelve grounds are listed, including for public health reasons, for judicial proceedings, for the protection or treatment of victims of abuse or neglect; for military personnel oversight; for employment reasons; and for reasons of unemployment compensation evaluations.[248] Thus, if a court

---

> *(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.*

45 CFR §160.103.

[242] Another amendment of the Ominibus package was in the context of breaches of data security, shifting the burden of proving that in the case of a breach, no harm had occurred to the provider (rather than requiring the claimant to prove that harm had occurred). See id.

[243] 45 CFR §160.103.

[244] Id.

[245] See 45 CFR §164.512 (https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=2112ccd8dc21de871c82cbfbd16564ec&mc=true&r=SECTION&n=se45.1.164_1512) (accessed 9 December 2017).

[246] 45 CFR §164.512(a).

[247] 45 CFR §164.512(b).

[248] 45 CFR §164.512 (c) – (l). See also Department of Health and Human Services, When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?

order from an administrative, civil, or criminal proceeding demands the release of health information, the covered entity may comply. The provisions of §164.512 specify, however, that any compliance with a demand should only release the data necessary and relevant to the request[249] – thus, compliance with a governmental demand for data within an administrative or civil case that is not accompanied by a court order is only permissible if there is a showing that the data subject's consent could not be attained and that an effort was made to notify the person about the request for data[250].

Where governmental demands are in the context of a **criminal proceeding**, non-warranted requests may be complied with for certain information, but not for DNA or other genetic information.[251] Where a court order accompanies the governmental request for data, the provisions noted earlier in this report regarding the legality of any court request (whether by subpoena, writ, or warrant) continue to govern.

Finally, it is important to reemphasize that State privacy laws may afford greater restrictions on governmental access to health data. The HIPAA requires a minimum level of privacy protection, but is not intended to be a national standard to the exclusion of State standards.

2.3.2. National Security Data Requests

The government may access data held by natural or legal persons for national security purposes to the extent set out in legislation. While the HIPAA permits health data to be given when the government makes a request based on national security interests[252], other laws give authority to the government to request more general data in pursuance of national security and/or foreign intelligence goals.

(https://www.hhs.gov/HIPAA/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html; viewed 9 December 2017).

[249] E.g., 45 CFR §164.512 (e)(i); 45 CFR §164.512 (f)(1)(C).

[250] E.g., 45 CFR §164.512 (e)(ii)(A), 45 CFR §164.512 (e)(iii)(A).

[251] See 45 CFR §164.512 (f)(ii)(2):

> *Permitted disclosures: Limited information for identification and location purposes. Except for disclosures required by law as permitted by paragraph (f)(1) of this section, a covered entity may disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:*
>
> *(i) The covered entity may disclose only the following information:*
>
> *(A) Name and address;*
> *(B) Date and place of birth;*
> *(C) Social security number;*
> *(D) ABO blood type and rh factor;*
> *(E) Type of injury;*
> *(F) Date and time of treatment;*
> *(G) Date and time of death, if applicable; and*
> *(H) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.*
>
> *(ii) Except as permitted by paragraph (f)(2)(i) of this section, the covered entity may not disclose for the purposes of identification or location under paragraph (f)(2) of this section any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.*

[252] 45 C.F.R. 164.512(k)(2):

> *"National security and intelligence activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333)."*

The National Security title of the United States Code[253], in combination with Executive Order 12333, gives the government the authority inter alia to collect information on individuals who may pose a threat to national security, by "any means" within Constitutional limits:

> *"(a) All means, consistent with applicable Federal law and this order, and with full consideration of the rights of United States persons, shall be used to obtain reliable intelligence information to protect the United States and its interests.*
> *(b) The United States Government has a solemn obligation, and shall continue in the conduct of intelligence activities under this order, to protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.*
> *(c) Intelligence collection under this order should be guided by the need for information to respond to intelligence priorities set by the President."*[254]

Since the expiration of Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act)[255], governmental collection of bulk data is no longer permissible. While the government can still request communications companies for data, this must be done through a warrant issued by the Foreign Intelligence Surveillance Act (FISA) Court. This court cannot authorize the collection of content data and are restricted to authorizing requests that are for counterterrorism or foreign intelligence purposes.

Even with these restrictions, there are legal questions as to the permissible scope of governmental data requests. In Carpenter v. United States[256], the question centers on whether government agents may gather mobile device location information without a search warrant. The questions raised in Apple Computer's refusal to comply with Federal Bureau of Investigation (FBI) demands to create a de-encryption code for a mobile device is another.

Carpenter v. United States

On 29 November 2017, the Supreme Court heard arguments on the need for a police warrant to seize and search mobile telephones, spurring numerous scholars and policy analysts to attempt to parce whether the individual's right to privacy should supercede the government's interest in protecting public security. In the case, the evidence the defendant's cellphone provider turned over to the police on the locations from which his calls were made was clearly incriminating. The legal issue was a Fourth Amendment question: had the police gathered the information legally, or did the lack of a judicial warrant authorizing the search action made it an illegal search and seizure, violating the defendant's constitutional rights and resulting in an exclusion of the use of any evidence so gathered from trial[257] (unless it could have been obtained by other legal means). While the trial and appellate courts held the evidence admissible as the result of a legitimate search of the seized phone, the Supreme Court

---

[253] 50 U.S.C. § 401 ff.

[254] Executive Order 12333, 1.1 Goals (available at https://www.gpo.gov/fdsys/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-sec401.htm).

[255] The Patriot Act expired in 2015, and was replaced by the and its replacement by the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA Freedom Act), Pub-Law 114-23. Section 215 of the Patriot Act was not included in the new law, although the government still has the competence to collect substantial amounts of data in the name of counter-terrorism, much of it prior to the need to have a warrant. See Caroline Lynch and Lara Flint, The USA FREEDOM Act Turns Two, Lawfare, 2 June 2017 (https://www.lawfareblog.com/usa-freedom-act-turns-two; viewed 9 December 2017).

[256] Timothy Ivory Carpenter v. USA, On Petition for a Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit, No. 16-402.

[257] Weeks v. United States, 232 U.S. 38/3 (1914) (case establishing the "exclusionary rule", holding that evidence obtained during an illegal search is not admissible at trial).

decision will signal a clear direction in the balancing of the individual and public interests in the digital age.

2016 Case of Apple Computer v. US

Widely discussed, Apple Computer's 2016 lawsuit against the FBI's demands for it to write a program to permit the government to unlock an iPhone used in a shooting addressed the questions of a third party's obligations to comply with a court order to create a product to permit federal investigators to search a mobile device. When faced with a judicial order compelling action, Apple Computer challenged the order in court as a violation of its right to freedom of expression. One of a number of similar challenges, the 2016 case ended when the FBI announced it did not require Apple's assistance. The legal question of the relationship between freedom of expression and governmental demands based on proffered security arguments therefore remains open.

III. ZUSAMMENFASSUNG

1. Tabellarische Übersichten

1.1. Datenportabilität

	Datenportabilität	**Herausgaberecht**	**Wiederverwendung des Resultats der Verarbeitung oder anonymisierter Daten**
EU	Ab Mai 2018	Ab Mai 2018	Nein
D	Nein (erst ab Mai 2018)	Nein (erst ab Mai 2018)	Nein
F	Ab Mai 2018	Ab Mai 2018	aB 2018: Soweit durch den Bearbeiter kein « enrichissement significatif » stattgefunden hat
S	Nein (erst ab Mai 2018)	Nein (erst ab Mai 2018)	Nein
JPN	Nein (acter diskutiert)	Nein	Nein
USA	Nein	Nicht ersichtlich	Nicht ersichtlich

1.2. Nutzungsrechte an digitalen Inhalten

	Schutz des Erstellers von Datenbanken	**Vertragsrecht**	**Weitere**
EU	Richtlinie 96/9/EG	Konsumentenschutzbestimmungen bei Verträgen über digitale Inhalte	---
D	Urheberrecht (Umsetzung Richtlinie 96/6/EG)	Konsumentenschutzbestimmungen bei Verträgen über digitale Inhalte (EU)	Allgemeines Wettbewerbsrecht: Schutz bei «unredlichem Erlangen der erforderlichen Unterlagen oder Kenntnisse»
F	Urheberrecht (Umsetzung Richtlinie 96/6/EG)	Konsumentenschutzbestimmungen bei Verträgen über digitale Inhalte (EU)	Allgemeine Wettbewerbsrechtliche «action en concurrence parasitaire» (Schadenersatz)
S	« Katalogsschutz » (Schutz der Zusammenstellung einer grossen Zahl von Informationen) und von Datenbanken (einer grossen Investition, Umsetzung Richtlinie 96/6/EG)	Konsumentenschutzbestimmungen bei Verträgen über digitale Inhalte (EU)	

	Schutz des Erstellers von Datenbanken	Vertragsrecht	Weitere
JPN	Ja, sofern Auswahl oder Zusammenstellung eine « Kreation » sind	Lizenzvereinbarungen scheinen bei Daten allgemein möglich	Schadenansprüche auch bei Verwertung nicht urheberrechtlich geschützten Datenbanken möglich. Wettbewerbsrechtliche Ansprüche möglich.

1.3. Zugang für den Staat

	Allgemein	Gesundheit	Statistik
D	--	Meldepflichten bei gewissen Krankheiten	Öffentliche Statistik gesetzlich angeordnet, inkl. Bestimmungen zur jeweiligen Meldepflicht
F		Umfassendes Zugangs- und Weiterverarbeitungsrecht des Staates	Allgemeine Zugangspflicht zu Gunsten des staatlichen statistischen Organs
S		-Meldepflichten bei bestimmten Krankheiten -Meldepflicht an nationales Register mit bestimmten Angaben -Informationspflichten gegenüber Gerichten und gewissen Behörden in Einzelfällen	Allgemeine Pflicht im «Statistik-Gesetz» zu Gunsten der verschiedenen staatlichen Statistikorganen
JPN			Allgemeine Auskunftspflicht gegenüber der Vorsteher einer administrativer Behörde, welche Erhebungen zu einer genehmigten «Grundsatzstatistik durchführt (Statistik Gesetz)
USA	Starker Schutz der Privatsphäre gemäss Verfassung	Zugang bei Gerichtsverfahren und zum Zweck der öffentlichen Gesundheit (detaillierte Bestimmungen	n/a

2. Beantwortung

1. Das Recht auf Datenportabilität wurde bislang lediglich im Europäischen Recht sowie (insbesondere in Umsetzung des Europäischen Rechts) in Frankreich gesetzlich verankert. In den USA wurde die Einführung eines Rechts auf Datenportabilität Ende 2016 erwogen, doch soweit ersichtlich sind seither keine weiteren Massnahmen ergriffen worden und es ist angesichts der aktuellen politischen Mehrheitsverhältnisse eher unwahrscheinlich, dass

diesbezüglich weitere Schritte getroffen werden. In Japan wurde mit der jüngeren Datenschutzrevision kein Recht auf Datenportabilität eingeführt, doch wird dies aktuell diskutiert.

A) In den untersuchten Rechtsordnungen besteht – abgesehen vom unter 1. erwähnten Recht auf Datenportabilität – kein Recht der Herausgabe von Daten zum Zweck der Weiterverwendung oder Nutzung.

B) Ein Recht auf Wiederverwendung des Resultats der Verarbeitung oder von anonymsierten Daten besteht soweit ersichtlich in keiner der untersuchten Rechtsordnungen. Eine gewisse Ausnahme ist ab Mai 2018 in Frankreich für nicht persönliche Daten vorgesehen, soweit die Verarbeitung keine «wesentliche Bereicherung» darstellt.

2. Das Europarecht sieht einen Schutz von Herstellern von Datenbanken vor, im schwedischen Recht ist dieser besonders ausgeprägt, und im japanischen Recht findet sich sowohl ein Schutz von Datenbanken als auch von Zusammenstellungen (*compilations*). Daneben bestehen soweit ersichtlich keine spezifischen Schutzvorschriften für Daten. In verschiedenen Rechtsordnungen erlaubt das Lauterkeitsrecht einen Schutz gegen das Ausnützen fremder Leistungen. Auf europäischer Ebene bestehen zudem Konsumentenschutzvorschriften spezifisch für Verträge über digitalen Inhalt.

3. Die untersuchten Rechtsordnungen variieren hinsichtlich der Grundsätze des staatlichen Zugangs zu Daten. Insbesondere im US-amerikanischen Recht ist auf eine umfassende Rechtsprechung hinzuweisen, welche auch auf den staatlichen Zugriff auf Daten anwendbar ist.

   Im Gesundheitsrecht sehen alle Rechtsordnungen Meldepflichten bzw. Rechte auf Zugang zu Informationen zu Zwecken der öffentlichen Gesundheit sowie im Rahmen von Gerichtsverfahren und zu Gunsten gewisser Behörden vor. Diese sind in der Regel sehr genau beschrieben.

   Im Bereich der Statistik haben die staatlichen Statistikorgane in Deutschland, Frankreich, Japan und Schweden weitgehende Zugangsrechte, wobei das jeweilige Ausmass in Deutschland für jede Statistik gesetzlich umschrieben wird. Im französischen und schwedischen Recht sind allgemeinere Zugangsrechte der statistischen Behörden vorgesehen. In Japan bezieht sich das Zugangsrecht nicht spezifisch auf Daten, sondern allgemein auf Material bzw. Dokumente.

Schweizerisches Institut für Rechtsvergleichung

Projektleitung und EU: Dr. Lukas Heckendorn Urscheler
Co-Leiter der wissenschaftlichen Abteilung

Deutschland: Dr. Johanna Fournier
Referentin für deutsches Recht

Frankreich:	Carole Viennet *Referentin für französischsprachige Rechtsordnungen*
Schweden	Henrik Westermark *Referent für skandinavisches Recht*
USA	PD Dr. Krista Nadakavukaren Schefer *Co-Leiterin der wissenschaftlichen Abteilung*
Japan	Dr. Lukas Heckendorn Urscheler, auf der Grundlage von Informationen von Wakako Oshima (Korrespondentin)