

Schutz sensibler Daten und Medien

Der gesetzliche Schutz besteht, doch es gibt wenig Praxis

Ursula Uttinger, lic. iur. / exec MBA HSG, Dozentin Hochschule Luzern sowie Datenschutzberatung, Zürich
Marc Ruef, Mitbegründer der Firma scip AG, Dozent an verschiedenen Hochschulen sowie Buchautor

Résumé: La protection des données personnelles est, aujourd'hui déjà, ancrée dans différentes lois. Toutefois, la question se pose régulièrement de savoir si elle suffit, en particulier dans le contexte du succès croissant des réseaux sociaux et de l'augmentation des attaques de pirates informatiques. En principe, on peut constater que la protection légale existe. Cependant, des plaintes sont très rarement déposées. C'est pourquoi il y a très peu de décisions de justice dans ce domaine, en Suisse.

Zusammenfassung: Der Schutz von Personendaten ist bereits heute in verschiedenen Gesetzen zu finden. Dennoch kommt immer mal wieder die Frage auf, ob dieser Schutz genügt, insbesondere auch durch die immer grössere Verbreitung von Social Media und durch die Zunahme von Hackerangriffen. Grundsätzlich lässt sich feststellen, dass der gesetzliche Schutz zwar besteht und Strafanzeigen immer wieder eingereicht werden; die privatrechtlichen Klagen, gestützt auf das Datenschutzgesetz, sind jedoch äusserst selten, weshalb es in der Schweiz auch kaum Gerichtsentscheide gibt.

I. Einleitung

1

Der Schutz der Privatsphäre ist in der Bundesverfassung^[11] in Art. 13 ausdrücklich geregelt und umfasst insbesondere auch den Schutz vor Missbrauch der persönlichen Daten. Wobei unter dem Begriff «Daten» Personendaten zu verstehen sind. Dazu gehören «alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen», wie dies in Art. 5 Bst. a DSG (Bundesgesetz über den Datenschutz)^[12] definiert ist. So können Personen auch aufgrund des Kontextes oder einer Kombination von Daten bestimmbar werden^[13].

2

Art. 5 Bst. c DSG definiert, was alles zu den «besonders schützenswerten Daten» gehört:

- «1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;»

3

Besonders schützenswert sind Daten, welche die Persönlichkeit betroffener Personen besonders stark berühren, weil sie einen Bezug zum Geheimbereich oder dem Privatleben haben oder das Ansehen und die soziale Geltung einer Person betreffen können^[14]. Mit der Revision des DSG gab es eine Erweiterung um die Ziffern 3 – genetische Daten – und 4 – biometrische Daten –, und in Ziffer 2 wurde die «Ethnie» ergänzt^[15]. Weiterhin als nicht besonders schützenswert gelten finanzielle Informationen

wie Einkommen- oder Vermögensverhältnisse; deren Schutz ist allenfalls in Spezialgesetzen wie dem Bankengesetz^[6] geregelt.

4

Mit der Medialisierung, insbesondere auch den sozialen Medien, stellt sich vermehrt die Frage, wie es um den Schutz der Personendaten steht. So hat die Kommission für Wirtschaft und Abgaben des Ständerates am 17. Oktober 2023 ein Postulat eingereicht, mit welchem der Bundesrat aufgefordert wird, aufzuzeigen, «wie der gesetzliche Schutz sensibler persönlicher Daten vor Veröffentlichungen dieser Daten durch soziale und private Medien verbessert werden kann»^[7].

5

Als Begründung wird im Postulat unter anderem angeführt, dass immer öfter durch illegale Handlungen wie Diebstahl durch Mitarbeitende oder Cyberangriffe Personendaten in den Besitz von Dritten gelangen.

6

Dazu kommt, dass Hackerangriffe zunehmen, wie der Beobachter bereits 2021 schrieb: «Hacker stürzen sich auf Schweizer Unternehmen»^[8]. Werden Forderungen nach Bezahlung eines Lösegeldes nicht erfüllt, landen Daten oft im Darknet – vgl. auch die Hackerangriffe auf NZZ/CH-Medien^[9] und Xplain^[10]. Solche Daten können dann von jedermann mit entsprechendem Wissen im Darknet gefunden werden.

II. Was ist das Darknet?

7

Grundsätzlich besteht das Internet aus drei Teilen: Dem allgemein bekannten Internet, dem Deep Web, welches ca. 90% ausmacht, und dem Darknet. Zum Deep Web gehören Firmendatenbanken, Dienste von Regierungen, Organisationen

oder Universitäten, Streaming-Server sowie Online-Speicher. Das Deep Web steht grundsätzlich allen offen, viele Inhalte sind jedoch geschützt. Das Darknet ist ein relativ kleiner Teil des Internets.^[11]

8

Das «Darknet» gilt als Dreh- und Angelpunkt für illegale Aktivitäten. Es handelt sich um eine Kommunikationsplattform, auf die nicht ohne weiteres zugegriffen werden kann. Entweder kommen eher unübliche Technologien zum Einsatz (z.B. Peer-to-Peer-Netze) oder es wird das Vorhandensein einer Vertrauensbeziehung, zum Beispiel in der Form eines Logins, vorausgesetzt.^[12]

9

Wenn heute der Begriff genutzt wird, wird er gerne dem Tor-Netzwerk gleichgesetzt. Dieses baut auf bestehenden Internet-Technologien auf, erweitert sie um ein mühsam nachvollziehbares Routing und zusätzliche Verschlüsselung. Privatsphäre, Abhörsicherheit und die Schwierigkeit einer Rückverfolgung werden dadurch erhöht.^[13]

10

Die grosse Herausforderung der professionellen Darknet-Analyse ist das Finden der relevanten Plattformen. Diese sind nicht oder nur beschränkt für die Öffentlichkeit zugänglich und meist eingeschworenen Subkulturen vorbehalten. Mit zusätzlichem Aufwand müssen diese infiltriert werden, was durch das Etablieren von fiktiven Personas geschieht.

III. Androhung einer Veröffentlichung

11

In den vergangenen Jahren wurde eine starke Zunahme von «Breaches» verzeichnet. Ransomware-Gangs kompromittieren

Unternehmen, um ihre Daten zu verschlüsseln und eine Freigabe zu erpressen^[14]. Viele Organisationen halten Backups bereit, wodurch dem illegalen Geschäftsmodell entgegengewirkt wird. Deshalb hat sich die sogenannte «Double Extortion» etabliert, bei der vor der Verschlüsselung die Daten durch die Angreifer heruntergeladen werden.

12

Professionelle Ransomware-Gangs betreiben Webportale, auf denen sie ihre Breaches ankündigen und auflisten. Den Opfern wird eine Frist gesetzt, bis wann die Zahlung durchgeführt werden muss. Falls diese nicht eingehalten wird, wird eine Veröffentlichung vorgenommen und «jeder» kann die gestohlenen Daten einsehen.

13

Journalisten und auf Darknet-Monitoring spezialisierte Firmen sind darum bemüht, die Legitimität und Tragweite dieser Leaks zu analysieren. Dabei werden die Leak-Seiten überwacht und neue Veröffentlichungen untersucht. Hierzu werden die veröffentlichten Daten heruntergeladen und die darin enthaltenen Dokumente geöffnet.

IV. Wie ist der Schutz der Daten heute?

14

Sowohl im Datenschutzgesetz (vgl. nachfolgenden Abschnitt), als auch im Strafgesetzbuch^[15], insbesondere Art. 143 StGB (Unbefugte Datenbeschaffung), Art. 179 ff. StGB (Strafbare Handlungen gegen den Geheim- oder Privatbereich), Art. 162 StGB (Geschäfts- und Fabrikationsgeheimnis), Art. 321 StGB (Berufsgeheimnis), Art. 321bis StGB (Berufsgeheimnis in der Forschung am Menschen), Art. 321ter StGB (Post- und Fernmeldegeheimnis), gibt es klare Regelungen, wie mit Daten umzugehen beziehungsweise was verboten ist. Weiter werden

Daten auch durch diversen Spezialgesetze, wie unter anderem in den Sozialversicherungsgesetzen – Art. 33 ATSG^[16] (Schweigepflicht) – oder dem Bankengesetz, welches per 1. Juli 2015 angepasst wurde und das Bankgeheimnis in Art. 47 BankG Abs. 1 um Bst. c erweitert^[17] hat, geschützt.

15

Art. 1 DSG umschreibt klar den Zweck des Gesetzes, nämlich «den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.» Dazu werden Grundsätze der Datenbearbeitung formuliert (Art. 6 und 8 DSG), den Bearbeitern Pflichten auferlegt (Art. 19 – 24 DSG) und Betroffenen Rechte gegeben (Art. 24 – 29 DSG sowie Art. 32 DSG).

16

Mit der Revision hat der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) mehr Kompetenzen erhalten, auch wenn er keine Bussen aussprechen kann, wie dies in der EU bzw. dem EWR gemäss Art. 58 DSGVO^[18] den staatlichen Datenschutzbehörden möglich ist.

17

Werden Personendaten entgegen den Grundsätzen des Datenschutzgesetzes bearbeitet, liegt eine Persönlichkeitsverletzung vor (Art. 30 Abs. 2 Bst. a DSG) und die betroffene Person kann gegen den Bearbeiter klagen.

18

Die Grundsätze umfassen folgende Punkte:

- Rechtmässige Datenbearbeitung
- Treu und Glauben
- Verhältnismässigkeit
- Zweckbindung
- Transparenz (enthalten in der Zweckbindung)

- Datensicherheit
- Datenrichtigkeit (umfasst Qualität der Daten)

19

In Bezug auf den Schutz der Daten stehen primär die Rechtmässigkeit und die Datensicherheit im Fokus. Die restlichen Grundsätze umfassen mehr die Art und Weise der Bearbeitung.

20

Die Rechtmässigkeit, geregelt in Art. 6 Abs. 1 DSG, verlangt von privaten Verantwortlichen, dass bei der Datenbearbeitung kein Verstoss gegen eine strafrechtliche oder vertragsrechtliche Norm wie die unbefugte Datenbeschaffung (Art. 143 StGB) oder absichtliche Täuschung eines Vertragspartners (Art. 28f ZGB^[191]) erfolgt^{[201], [211]}. Sind Daten einmal gestohlen, bleiben diese Daten illegal^[221]. Eine Verwertung solcher Daten darf nur zur Aufklärung schwerer Verbrechen erfolgen (Art. 141 Abs. StPO^[231]). Dies wurde vom Bundesgericht auch wiederholt im Zusammenhang mit Dashcam-Aufnahmen bestätigt^[241].

21

Bezüglich von Daten aus dem Darknet müsste man grundsätzlich hinterfragen, ob diese Daten gestohlen sind. Kommt man zu diesem Schluss, ist jede weitere Bearbeitung ebenfalls nicht rechtmässig.

22

Bearbeiten im Sinne des Datenschutzgesetzes ist bekanntlich breit zu verstehen: «*Bearbeiten*: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten» (Art. 5 Bst. d DSG).

Zusammengefasst bedeutet dies also, dass gestohlene Daten nicht bearbeitet werden dürften. Wobei Art. 2 DSG den Anwendungsbereich definiert (Abs. 1) und zugleich auch einschränkt (Abs. 2). Gemäss Art. 2 Abs. 2 Bst. a ist das DSG nicht anwendbar, auf «Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden» (vgl. unten).

V. Datensicherheit

Die Datensicherheit ist in Art. 8 DSG sehr allgemein formuliert: Durch geeignete technische und organisatorische Massnahmen soll eine dem Risiko angemessene Datensicherheit gewährleistet werden. In der Datenschutzverordnung^[251] werden dann diverse technische und organisatorische Massnahmen aufgezählt. Wichtig ist dabei, dass der Schutzbedarf der Daten vorgängig definiert und dann, entsprechend den Risiken, angemessene Massnahmen getroffen werden^[261]. Ein absoluter Schutz der Daten kann aber auch mit grösstem Aufwand nicht gewährleistet werden. Dies zeigen auch die Auswirkungen verschiedener Cyberangriffe.

VI. Datenhehlerei

Im oben genannten Postulat 23.4322 wird der Begriff der Datenhehlerei aufgenommen. Bereits am 8.12.2022 hat Ständerat Baptiste Hurni die Motion «Es ist wichtig, die Hehlerei mit digitalen Daten zu bestrafen»^[271] eingereicht, nachdem im Kanton Neuenburg Daten von Patientinnen und Patienten gestohlen worden waren. Der Bundesrat lehnte die Motion damals ab mit Hinweis auf andere Tatbestände im Strafgesetzbuch sowie das

Übereinkommen des Europarates zu Cyberkriminalität. In der Folge wurde die Motion zurückgezogen. Am 12.3.2013 wurde von der damaligen Nationalrätin Viola Amherd eine weitere Motion eingereicht: «Anpassung des Hehlerei-Tatbestandes im Strafgesetzbuch»^[28]. Im BankG kam es dann zu einer Anpassung (vgl. vorne Rn. 14 und Fussnote 17). Schon damals meinte der Bundesrat, ein weiterer Tatbestand im Strafgesetzbuch sei nicht zwingend und wiederholte dies nun wieder, denn die geltende materielle Rechtslage sei grundsätzlich ausreichend, um eine weitere Verwendung illegal erworbener Daten zu erfassen.

26

Im Gegensatz zur Schweiz kennt Deutschland den Straftatbestand der Datenhehlerei (§ 202d StGB Deutschland – in Kraft seit dem 18. Dezember 2015). Darunter versteht man «Daten, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen»; wobei diese Strafnorm nicht anwendbar ist, wenn es um die Nutzung ausschliesslich für eine Verwertung in einem Besteuerungsverfahren geht (§ 202 Abs. 3 Ziffer 1).

27

Diese Strafnorm führte einerseits zu grosser Kritik, da dieser Strafartikel einerseits «imaginäre Rechte schütze» und «handwerklich fehlerhaft» sei^[29], andererseits zu Verunsicherung bei den Medienschaffenden Anlass gebe. Das Bundesverwaltungsgericht entschied^[30] auf eine Verfassungsbeschwerde hin, eingereicht durch die Gesellschaft für Freiheitsrechte^[31], dass der Straftatbestand der Datenhehlerei keine Anwendung auf Journalisten findet, die mit geleakten Daten arbeiten^{[32], [33]}.

VII. Medienprivileg

28

Das Bundesgesetz über den Datenschutz (DSG) kennt einzelne Spezialbestimmungen für Journalistinnen und Journalisten bzw. für Medien. Es handelt sich dabei um ein Medienprivileg.^[34], ^[35]

29

Gemäss Art. 27 DSG (Einschränkung des Auskunftsrechts für Medien) wird das Auskunftsrecht gegenüber den Medien eingeschränkt. Bereits bei der Informationspflicht von Art. 19 DSG wird in Bezug auf Ausnahmen der Informationspflicht in Art. 20 DSG auf Art. 27 verwiesen. Mit anderen Worten: Einerseits müssen Medien nicht über eine Datenbearbeitung informieren und andererseits haben betroffene Personen kein Auskunftsrecht, sofern die Daten einzig für die

- Veröffentlichung
- im redaktionellen Teil
- eines periodisch erscheinenden Mediums

genutzt werden. Gesetzliche Gründe für die Verweigerung einer Auskunft können der Schutz der Informationsquelle oder des Entwurfsstatus der Publikation sein sowie eine Gefährdung der freien Meinungsbildung des Publikums.^[36]

30

Weiter können Medienschaffende, gestützt auf Art. 31 Abs. 2 Bst. d DSG, ein überwiegendes Interesse als Rechtfertigungsgrund für eine Persönlichkeitsverletzung anbringen, sofern im beruflichen Kontext die Daten ausschliesslich zur Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums dienen. Damit ist nicht die Veröffentlichung selbst gemeint – dafür braucht es einen eigenen Rechtfertigungsgrund (vgl. hinten) – sondern die Nutzung, Bearbeitung vor oder nach der Publikation. Falls es zu keiner Publikation kommt, kann alternativ auch mit dem

persönlichen Arbeitsinstrument argumentiert werden.^[37]

31

Die Medien nehmen in Bezug auf den Datenschutz eine Sonderstellung ein, die sich aus dem verfassungsrechtlichen Informationsauftrag herleiten lässt.^[38] Dieser spielt dabei eine zentrale Rolle: In Art. 17 BV ist die Medienfreiheit verankert. Gerade der Europäische Menschenrechtsgerichtshof (EGMR) befasst sich regelmässig mit den Medien und dem Recht auf Meinungsäusserungsfreiheit (siehe dazu die jährliche Entscheidübersicht von Franz Zeller zum Verfassungsrecht und der EMRK, zuletzt in [«medialex 10/23»](#)). Den Medien wird dabei die Rolle als «Wachhund der Demokratie» zugeteilt,^[39] wobei auch Grundrechte, wie beispielsweise die Medienfreiheit, eingeschränkt werden können. Voraussetzung dafür ist, dass die Einschränkung in einem Gesetz vorgesehen ist, diese durch öffentliches oder privates Interesse gerechtfertigt scheint, verhältnismässig ist und der Kerngehalt des Grundrechts unberührt bleibt (Art. 36 BV).

VIII. Daten aus dem Darknet und Medienschaffende

32

Regelmässig findet man im Darknet Daten, nachdem Unternehmen gehackt worden sind. Diese Daten sind für jedermann zugänglich, der sich im Darknet auskennt, und können gefunden werden. Spezialisierte Journalisten wie Otto Hostettler^[40] publizieren regelmässig über Cyber-Vorfälle. Dabei stellt sich immer wieder die Frage: Nennung von betroffenen Personen oder Anonymisierung? Dasselbe gilt auch, wenn Whistleblower mit Medienschaffenden in Kontakt treten und Personen namentlich anschwärzen.

33

Eine Nennung von Personennamen kann eine Persönlichkeitsverletzung im Sinne von Art. 28 ff. ZGB darstellen; dabei ist auch die sogenannte Sphärentheorie^[41] zu beachten: Es ist zu differenzieren zwischen der Intim- oder Geheimsphäre (die nicht publik sein soll), der Privatsphäre (nur geteilt mit ausgewählten Personen, wie Freunden und Familie) sowie der öffentlichen Sphäre (faktisch jedermann zugänglich)^[42].

34

Medienschaffende müssen entscheiden, ob sie die Daten einzig als persönliches Arbeitshilfsmittel nutzen wollen, die Daten nur in anonymisierter Form nutzen oder ob ihnen ein Rechtfertigungsgrund für die Veröffentlichung zusteht (Art 28 Abs. 2 ZGB).

35

Wie bereits oben festgehalten, ist das DSG nicht anwendbar, wenn ein Medienschaffender die Daten für sich für die eigene Recherche nutzt. Denn dann handelt es sich um ein persönliches Arbeitsinstrument. Bereits in der Botschaft zum DSG vom 19. Juni 1992 steht ausdrücklich: «Notizen, die jemand zwar bei der Ausübung seines Berufs, aber nur als Arbeitshilfe zum persönlichen Gebrauch macht, etwa zur Gedächtnisstütze, fallen nicht unter das Gesetz.»^[43] Mit der Revision des DSG hat sich hier materiell nichts geändert, es gab bloss eine rein redaktionelle Anpassung^[44].

36

Werden die Daten anonymisiert genutzt, unterstehen sie ebenfalls nicht dem DSG, da eine Bestimmbarkeit der betroffenen Person fehlt. In der Praxis entscheiden sich Medienschaffende oft, Fälle anonym zu publizieren^{[45], [46], [47]} bzw. einzig die angegriffenen Unternehmen zu nennen.

37

Sollen Personen genannt werden, dürfte in den meisten Fällen ein überwiegendes öffentliches Interesse der Rechtfertigungsgrund sein^[48]. Das Bundesgericht hat wiederholt festgehalten, dass Medien «einen Informationsauftrag» haben^[49]. Bereits 1911 hat sich das Bundesgericht mit der Pressefreiheit auseinandergesetzt und die Aufgaben der Presse im Interesse eines öffentlichen Meinungsaustausches festgehalten^[50]. Diese Haltung hat es 1996 in BGE 122 III 449 bestätigt.

38

Wie heikel die Nennung von Namen ist, zeigt auch der Fall der Luzerner Hackerin Tilli Kottmann, bekannt unter Maia Arson Crimew, die vom EDÖB kontaktiert wurde, nachdem sie eine Flugverbotsliste von Terrorverdächtigen der USA gehackt hatte^[51]. In diesem Schreiben wird sie darauf hingewiesen, dass «die Bekanntgabe dieser Liste an Dritte, und damit auch an Journalisten, [.....] rechtswidrig» ist^[52].

39

Das Postulat 23.4322 fordert auch eine Prüfung, ob «in welchen Fällen überhaupt illegal erlangte Informationen aller Art veröffentlicht werden dürfen, respektive in welchen Sachverhalten das öffentliche Interesse gegenüber dem privaten Interesse, dass die illegal erlangten Daten nicht veröffentlicht werden dürfen überwiegt und in welchen Fällen auf eine Strafbarkeit verzichtet werden könnte».

40

Eine solche Prüfung erfolgt bereits heute^[53]. Das Bundesgericht hält dazu fest, dass «Medien nicht ohne triftigen Grund in die persönlichen Verhältnisse Einzelner» eingreifen dürfen. «Andererseits hat der einzelne Rechtsgenosse gewisse durch das öffentliche Interesse hinreichend gerechtfertigte Eingriffe in

seine persönlichen Verhältnisse zu dulden»^[54].

41

Im Postulat wird zudem von privaten und sozialen Medien gesprochen. Sowohl im Straf- als auch Datenschutzgesetz wird nicht differenziert zwischen privaten und staatlichen Medien. Umgangssprachlich versteht man unter Medien Radio, Fernsehen, Zeitungen und Zeitschriften. Doch auch soziale Medien gehören dazu: Im Zusammenhang mit Art. 28 StGB^[55] (Strafbarkeit der Medien) wird der Begriff der Medien weit ausgelegt und Social Media werden ausdrücklich als Teil der Medien betrachtet^{[56], [57], [58]}. 2002 hielt das Bundesgericht fest, dass der Begriff der Medien weit zu interpretieren sei^[59], und 2021 meint das Bundesgericht, dass Social Media in den verschiedensten Formen vorkommen, und: «Ihr Inhalt reicht von journalistischen Beiträgen, Kommentaren aus der Leserschaft bis hin zur blossen Alltagskommunikation in Wort, Schrift, (bewegtem) Bild und Ton (vgl. Nachfolgebericht des Bundesrates, a.a.O., S. 6 ff.). Die Weite des Medienbegriffs führt allerdings nicht dazu, Social Media gemeinhin als “Medium” zu qualifizieren»^[60]. Es muss in jedem Einzelfall geprüft werden, inwiefern das Medienprivileg auf Social Media anwendbar ist, auch wenn das Bezirksgericht Zürich klar festhält, dass «Twitter genauso wie ein Blog auf der Website des Schweizer Fernsehens als Medium im Sinne von Art. 28 StGB zu behandeln»^[61] sei. Diese weite Interpretation zeigt sich auch in einem Urteil des Obergerichts des Kantons Zürich, welches den Betreiber eines Youtube-Kanals auch als Medienschaffenden versteht^{[62], [63]}. Auch wenn es sich vorliegend um strafrechtliche Urteile handelt, kann diese Interpretation auch im Datenschutz angewendet werden.

IX. Fazit

42

Personendaten werden durch diverse Gesetzesbestimmungen geschützt. Im Alltag dürften weniger die fehlenden gesetzlichen Grundlagen eine Herausforderung sein als vielmehr der Wille und das Wissen von betroffenen Personen. Strafanzeigen werden zwar immer wieder eingereicht; die privatrechtlichen Klagen, gestützt auf das Datenschutzgesetz, sind jedoch äusserst selten. Dies dürfte auch damit zusammenhängen, dass die Begriffe wie beispielsweise Verhältnismässigkeit, Treu und Glauben zu interpretieren und je nach Anwendungsfall unterschiedlich gehandhabt werden.

43

Weitere gesetzliche Bestimmungen dürften daran nichts ändern, vielmehr liegt es an der Sensibilisierung der Nutzerinnen und Nutzer im Umgang mit Daten aus nicht eindeutig identifizierbaren Quellen.

Fussnoten:

1. SR 101. [↑](#)
2. SR 235.1. [↑](#)
3. Beat Rudin, Art. 5 N 10 in SHK Datenschutzgesetz, 2. Auflage, Bern, 2023. [↑](#)
4. Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II, 446. [↑](#)
5. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung

weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 7020. [↑](#)

6. SR 952.0. [↑](#)

7. Postulat 23.4322 Handhabung der weiteren Verwendung illegal erworbener Daten. [↑](#)

8. <<https://www.beobachter.ch/digital/sicherheit/immer-mehr-angriffe-hacker-sturzen-sich-auf-schweizer-firmen-349877>> 14. September 2024. [↑](#)

9. <<https://www.nzz.ch/technologie/kriminelle-hacker-greifen-die-nzz-an-und-erpressen-sie-cyberangriff-ransomware-ld.1778725>> 14. September 2024. [↑](#)

10. <<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-100315.html> > 14. September 2024. [↑](#)

11. <<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deepweb.html>> 14. September 2024. [↑](#)

12. <<https://www.scip.ch/?labs.20160114>> 14. September 2024. [↑](#)

13. <<https://www.wired.co.uk/article/what-is-the-dark-web-how-to-access>> 14. September 2024. [↑](#)

14. <<https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals>> 6. Juli 2024. [↑](#)

15. SR 311.0. [↑](#)

16. SR 830.1. [↑](#)

17. BBl 2014 6236 f. Siehe dazu ausführlich David Zollinger, [Die Verwendung von Bankdaten durch Medienschaffende, medialex 06/22](#), [↑](#)

18. Verordnung (EU) 2016/679. [↑](#)
19. SR 210. [↑](#)
20. Bruno Baeriswyl, Art. 6 Rz 13, SHK DSG 2013. [↑](#)
21. David Rosenthal, aArt. 4 RZ, Handkommentar zum Datenschutzgesetz, Zürich 2008. [↑](#)
22. Andrea Opel, Wider die Amtshilfe bei Datenklau: Gestohlene Daten sind gestohlene Daten, in: Jusletter 23. November 2015. [↑](#)
23. SR 312.0. [↑](#)
24. 6B_1188/2018 vom 26. September 2019; 6B_810/2020 vom 14. September 2020. [↑](#)
25. SR 235.11. [↑](#)
26. Bruno Baeriswyl, Art. 8 Rz 1 ff., SHK DSG 2013. [↑](#)
27. Motion 22.4325 Es ist wichtig, die Hehlerei mit digitalen Daten zu bestrafen von, eingereicht von Baptiste Hurni. [↑](#)
28. Motion 12.3123 Anpassung des Hehlereitattbestandes im Strafgesetzbuch, eingereicht von Viola Amherd. [↑](#)
29. Stuckenberg Carl-Friederich, Dder missratene Tatbestand der neuen Datenhehlerei (§ 202d StGB) in ZIS 08/2016, S. 529 ff. [↑](#)
30. Bundesverfassungsgericht 1 BvR 2821/16. [↑](#)
31. < <https://freiheitsrechte.org/>> 25. Juli 2024. [↑](#)
32. < <https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-datenhehlerei-bverfg>> 23. Juli 2024. [↑](#)

33. <
<https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/verfassungsgericht-staerkt-pressefreiheit>> 23. Juli 2024. [↑](#)
34. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, vom 15. September 2017, BBl 2017 7053. [↑](#)
35. Christoph Born, Andreas Blattmann, Simon Canonica, Peter Studer: Medienrecht der Schweiz IN A NUTSHELL, S. 73, 2. Auflage, Zürich/St. Gallen 2023. [↑](#)
36. Martin Steiger, Kommentierung zu Art. 27 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 28.08.2023: <<https://onlinekommentar.ch/de/kommentare/dsg27>> 6. Juli 2024), N3 ff. [↑](#)
37. Monika Pfaffinger, Art. 31 Rz 76 Datenschutzgesetz,. [↑](#)
38. Rolf H. Weber, Medien im Spannungsfeld von Informationsauftrag und Datenschutz, in: Jusletter 8. Mai 2017, Rz 49. [↑](#)
39. Rudolf Mayer von Baldegg, Dominique Strebel, Medienrecht für die Praxis, Saldo Ratgeber, S. 10, 5. Auflage, Zürich 2018. [↑](#)
40. Otto Hostetter, Redaktor/Reporter beim Beobachter, Autor von div. Büchern zu Cyberkriminalität, u.a. «Darknet: Die Schattenwelt des Internets» oder zusammen mit Abdelkader Cornelius «Underground Economy: Wie Cyberkriminelle Wirtschaft und Staaten bedrohen» [↑](#)
41. BGE 118 IV 45 ff. oder auch BGE 140 III 28 ff. [↑](#)
42. Mayer von Baldegg/Strebel S. 170. [↑](#)

43. BBl 1988 II 441. [↑](#)
44. BBl 2017 7012. [↑](#)
45. Otto Hostettler, Hacker stürzen sich auf Schweizer Firmen, Beobachter, veröffentlicht 6. Oktober 2021 < <https://www.beobachter.ch/digital/sicherheit/immer-mehr-angriffe-hacker-sturzen-sich-auf-schweizer-firmen-349877>> 28. Juli 2024. [↑](#)
46. Otto Hostettler, Jetzt wird's richtig gefährlich, Beobachter, veröffentlicht am 12. Mai 2022 < <https://www.beobachter.ch/multimedia/digital/jetzt-wirds-richtig-gefahrlich-379199>> 28. Juli 2024. [↑](#)
47. Otto Hostettler, Hacker erpressen Bernina und fordern 1.3 Millionen, Beobachter, veröffentlicht am 28. April 2023 < <https://www.beobachter.ch/digital/cybercrime-ransomware-banden-erpressen-nahmaschienenhersteller-bernina-und-fordern-losegeld-597553>> 28. Juli 2024. [↑](#)
48. Born, Blattmann, Canonica, Studer, S. 29. [↑](#)
49. BGE 122 III 449 – E 3b. [↑](#)
50. BGE 37 I 381. [↑](#)
51. < <https://www.zentralplus.ch/technologie-digitales/luzerner-hackerin-veroeffentlicht-flugverbotsliste-der-usa-2513319/>> 1. August 2024. [↑](#)
52. Schreiben des EDÖB an Maia Arson Kottmann vom 7. Februar 2023, S. 2. [↑](#)
53. Christoph Born, Andreas Blattmann, Simon Canonica, Peter Studer: Medienrecht der Schweiz IN A NUTSHELL, S. 29, 2. Auflage, Zürich/St. Gallen 2023. [↑](#)

54. BGE 95 II 481 E7. [↑](#)
55. SR 311.0. [↑](#)
56. Patrick Uhrmeister, Catherine Konopatsch, Art. 28 Rz 2, StGB Annotierter Kommentar, Bern 2020. [↑](#)
57. Stefan Rechsel, Marc Jean-Richart-Dit-Bressel, Art. 28 Rz 3 in: Schweizerisches Strafgesetzbuch, Praxiskommentar, Zürich 2021. [↑](#)
58. Andreas Donatsch, Artl 28 Rz 2StGB/JStGB Kommentar, OFK-Orell Füssli Kommentar, 21. Auflage, Zürich 2022. [↑](#)
59. BGE 128 IV 65 E 5c “La notion de presse doit être comprise dans un sens large (cf. DENIS BARRELET, Droit de la communication, Berne 1998, p. 332) ». [↑](#)
60. BGE 147 IV 65 [↑](#)
61. BezGer ZH GG1500250-L v. 26.1.2016. [↑](#)
62. Obergericht Zürich, Urteil SU230054 vom 16. April 2024 [↑](#)
63. <https://www.nzz.ch/zuerich/zuerich-obergericht-bestaetigt-freispruch-von-corona-skeptiker-daniel-stricker-ld.1834420> [↑](#)



Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).