Jusletter

Nutzung von Daten aus dem Darknet

Insbesondere mit Blickwinkel auf den Datenschutz

Autoren/Autorinnen: Ursula Uttinger / Marc Ruef
Beitragsart: Beiträge
Rechtsgebiete: Datenschutz
DOI: 10.38023/df607a98-14c2-4fb4-8b1a-e575d011744e
Zitiervorschlag: Ursula Uttinger / Marc Ruef, Nutzung von Daten aus dem Darknet, in: Jusletter 23. September 2024

Ein Hackerangriff ist heute keine Seltenheit mehr. Betroffene werden erpresst – einerseits um wieder Zugang zu den Daten zu haben, andererseits damit Daten nicht im Darknet veröffentlicht werden. Finden Medienschaffende Daten im Darknet, sind die Persönlichkeitsrechte und der Datenschutz zu beachten.

Inhaltsverzeichnis

[1] In den vergangenen Jahren wurde Unternehmen vermehrt von Hackern angegriffen. Breite Bekanntheit haben die Fälle der NZZ/CH-Medien[1] und von Xplain[2]. Daneben gibt es noch viele weitere Fälle, wie der Beobachter bereits 2021 schrieb: «Hacker stürzen sich auf Schweizer Unternehmen»[3]. Oft werden keinen Namen von Betroffenen genannt – seien dies Unternehmen (v.a. juristische Personen) oder betroffene natürliche Personen. Es kann aber vorkommen, dass im Zusammenhang mit solchen Medienartikeln Personen benannt werden oder

erkennbar sind. Daraus ergeben sich verschiedene juristische Fragestellungen, unter anderem auch datenschutzrechtliche.

1. Medienprivileg

[2] Das Bundesgesetz über den Datenschutz (DSG) kennt einzelne Spezialbestimmungen für Journalistinnen und Journalisten bzw. für Medien. Es handelt sich dabei um ein Medienprivileg[4, 5]:

[3] 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 DSG 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.[6] 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. unten) – sondern die Nutzung, Bearbeitung vor oder nach der Publikation. Falls es zu keiner Publikation kommt, kann alternativ auch mit dem persönlichen Arbeitsinstrument argumentiert werden.[7]

[4] Grundsätzlich haben Medien eine Sonderstellung in Bezug auf den Datenschutz, der sich aus dem verfassungsrechtlichen Informationsauftrag herleiten lässt.[8] Dieser Informationsauftrag der Medien spielt dabei eine zentrale Rolle und ist in Art. 17 BV als «Medienfreiheit» verankert. Gerade der Europäische Menschengerichtshof (EGMR) befasst sich regelmässig mit den Medien und der Meinungsäusserungsfreiheit. Den Medien wird dabei die Rolle als «Wachhund der Demokratie» zugeteilt;[9] 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).

[5] Auch die europäische Datenschutzgrundverordnung kennt ein Medienprivileg: In Art. 85 DSGVO sind Abweichungen unter anderem bezüglich der Grundsätze und der Rechte Betroffener vorgesehen. Diese Ausnahmen werden unter anderem auch mit der Meinungsäusserungsfreiheit und der Informationsfreiheit begründet.[10]

2. Recherche im Darknet

[6] Das Medienprivileg spielt insbesondere dort eine wichtige Rolle, wo es um die Frage geht, ob in einem Medium veröffentlichte Daten dem Datenschutz unterstehen.[11] Nach einer Veröffentlichung kann die informationelle Selbstbestimmung durch die betroffene Person nicht mehr ausgeübt werden, und auch die Ansprüche aus Datenschutzverletzungen – Verbot einer Bearbeitung oder Weitergabe – sind hinfällig. Betroffene Personen können

sich nach einer Veröffentlichung nur noch auf Basis von Art. 28ff. ZGB gegen eine widerrechtliche Verletzung der Persönlichkeit zur Wehr setzen. Dabei können sie bei Gericht beantragen, die Verletzung zu verbieten, zu beseitigen und die Widerrechtlichkeit derselben festzustellen. Sie können zudem eine Berichtigung oder Gegendarstellung verlangen. [12]

[7] Im Rahmen von Recherchen spielt das Darknet für Journalistinnen und Journalisten eine immer bedeutendere Rolle. Oft erhalten diese von Whistleblowern einen Hinweis und Informationen finden sich im Darknet. Dabei stellt sich die Frage: Wie sieht es mit dem Datenschutz im Darknet aus. Doch was ist das Darknet?

[8] Grundsätzlich besteht das Internet aus drei Teilen: Dem allgemein bekannten Internet, auch Clear Web genannt, sowie dem Deep Web, welches ca. 90% ausmacht. 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. Der dritte und relativ kleine Teil ist das Darknet. [13]

2.1. Definition des Darknets

[9] Das «Darknet» gilt als Dreh- und Angelpunkt für illegale Aktivitäten im digitalen Zeitalter. Bemüht man das Internet, finden sich verschiedene Definitionen, die sich teilweise widersprechen. Auf den gemeinsamen Nenner reduziert handelt es sich beim Darknet um eine Kommunikationsplattform, auf die nicht ohne weiteres zugegriffen werden kann. Entweder kommen eher unübliche Technologien zum Einsatz, wie dies beispielsweise bei Peer-to-Peer-Netzen zum Tausch von Musik und Filmen der Fall ist. Andererseits viel wichtiger aber ist oftmals das Vorhandensein einer Vertrauensbeziehung. Diese kann in der Form einer Registrierung und damit einhergehendem Login gegeben sein. [14]

[10] Das Darknet ist also grundsätzlich nicht primär von der Wahl der Technologien abhängig. Wenn gemeinhin der Begriff genutzt wird, wird er gerne mit dem Tor-Netzwerk assoziiert. Dieses baut auf bestehende Internet-Technologien auf und erweitert diese um komplexes Onion-Routing und zusätzliche Verschlüsselungsmechanismen. Privatsphäre, Abhörsicherheit und die Schwierigkeit einer Rückverfolgung werden dadurch massgeblich erhöht. Mittels Tor lassen sich beliebige Dienste betreiben, wie wir sie auch vom regulären Internet kennen: Webseiten, Mailserver und Chat-Systeme. Sie alle können für das Orchestrieren, Tauschen und Verkaufen von illegalen Gütern zum Einsatz kommen. [15]

2.2. Plattformen finden und infiltrieren

[11] 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 Plattformen dann infiltriert werden, was oftmals durch das Etablieren von fiktiven Personas, sogenannten *Legenden*, geschieht. Die Wahl einer *Legende* orientiert sich in erster Linie am Szenario: Als wen man sich ausgeben muss, ist unterschiedlich, je nachdem ob man einen Markt für Drogen, Waffen oder Daten infiltrieren möchte.

[12] Das Ausarbeiten der *Legende* muss mit grösster Sorgfalt erfolgen, um Fallstricke, nicht bewältigbare Aufwände und Widersprüche verhindern zu können. Die Wahl des Geschlechts, der Herkunft und der Sprachfähigkeiten sind nur einige wenige Eigenschaften, die es geschickt zu definieren gilt. Dabei versucht man, möglichst nahe an der Realität zu bleiben, um wenig «lügen» zu müssen. Denn das Aufrechterhalten eines Lügenkonstrukts ist aufwändig und fehleranfällig. Dennoch darf die Legende nicht zu sehr der Wahrheit

entsprechen, um eine gewisse Entkoppelung des Analysten und damit das Verhindern der Deanonymisierung gewährleisten zu können.

3. Androhung einer Veröffentlichung

[13] In den vergangenen Jahren wurde eine starke Zunahme von «Breaches» verzeichnet. Professionelle Ransomware-Gangs kompromittieren reihenweise Unternehmen. In erster Linie werden die Daten verschlüsselt, um von den Opfern eine Freigabe zu erpressen[16]. Da viele Organisationen mit Backups aufwarten und dadurch diesem lukrativen Geschäftsmodell entgegenwirken können, hat sich die sogenannte «Double Extortion» etabliert: Bevor die Daten verschlüsselt werden, werden diese durch die Angreifer heruntergeladen. Will ein Kunde den Zugriff auf die Daten nicht freikaufen (z.B., weil er das Problem anderweitig lösen kann), wird mit der Veröffentlichung der Daten gedroht. Gerade wenn es sich um geheime, sensitive oder sensible Daten handelt, kann so dennoch eine Erpressung durchgesetzt werden.

[14] Professionelle Ransomware-Gangs betreiben Webportale, auf denen sie ihre durchgesetzten Breaches wie Trophäen führen und anstehende Leaks ankündigen. Den Opfern wird eine Frist gegeben, bis wann die Transaktion durchgeführt werden muss. Falls diese nicht eingehalten wird, wird eine Veröffentlichung vorgenommen und «jeder» kann die gestohlenen Daten einsehen. Mit weitsichtigem Verhandlungsgeschick kann man eine solche Veröffentlichung verhindern oder wenigstens hinauszögern. Amateuren ist vom Eigenversuch abzuraten, da üblicherweise eine Vielzahl an taktischen Fehlern begangen wird.[17]

[15] Journalistinnen und Journalisten und auf Darknet-Monitoring spezialisierte Firmen sind darum bemüht, die Legitimität und Tragweite dieser Leaks zu analysieren. Zu diesem Zweck werden die Leak-Seiten überwacht und neue Veröffentlichungen untersucht. Traditionell werden hierzu die veröffentlichten Daten heruntergeladen und die darin enthaltenen Dokumente geöffnet. Die Verfügbarkeit und Erreichbarkeit der Leak-Portale ist oftmals sehr schlecht, Seiten sind plötzlich nicht mehr verfügbar und Downloads brechen mittendrin ab, weshalb allein das Herunterladen manchmal mehrere Wochen erfordern kann.

4. Gehackt – was nun?

[16] Mit der Revision des Datenschutzgesetzes sind Unternehmen neu verpflichtet, einen Cybervorfall zu melden (Art. 24 DSG), sofern dieser «zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte Betroffener führt.» Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat dazu Informationen veröffentlicht.[18] Eine Herausforderung ist dabei die Definition des «Hohen Risikos», welche dem Geschädigten obliegt.

[17] Das Meldeportal des EDÖB zur Meldung von Datensicherheitsverletzung[19] kann als Hilfestellung genutzt werden. Diese Punkte werden aufgezählt als eine Folge der Datensicherheitsverletzung (mit Beispielen ergänzt, die nicht gerade auf der Hand liegen):

- Identitätsdiebstahl – z.B. im Netz wird die Identität missbraucht;
- Gefährdung der körperlichen Unversehrtheit oder des Lebens – z.B. kann es dies geben, wenn Daten einer Gesundheitseinrichtung verschlüsselt werden und Operationen/Behandlungen nicht durchgeführt werden können;
- Verlust des Arbeitsplatzes – z.B., weil Informationen an die Öffentlichkeit gelangen, die bis anhin nur einem kleinen Kreis bekannt waren, und gegen die gängigen Moralvorstellungen verstossen;
- Finanzieller Schaden;

- Verleumdung, Rufschädigung – gerade mit KI kann dies schnell erreicht werden: Daten werden mit falschen Informationen vermischt;
- Verweigerung der Dienstleistung;
- Betrug;
- Offenlegung von Amts- oder Berufsgeheimnissen;
- Diskriminierung;
- Sonstige wirtschaftliche Nachteile;
- Blossstellung;
- Sonstige soziale Nachteile.

[18] Dennoch bleibt es Sache des geschädigten Unternehmens, zu definieren, ob der Vorfall ein hohes Risiko bedeutet.

[19] Nebst der Meldepflicht an den EDÖB ist auch noch abzuwägen, ob die betroffenen Personen zu informieren sind (Art. 24 Abs. 4 DSG). Diese Meldung erfolgt entweder auf Verlangen des EDÖB oder wenn es zum Schutz Betroffener notwendig ist. Eine solche Information ermöglicht es betroffenen Personen zu reagieren.[20] Die Information kann eingeschränkt, aufgeschoben oder es kann ganz darauf verzichtet werden, entweder aufgrund einer Interessensabwägung zugunsten Dritter oder bei Bundesorganen, wenn dies aufgrund überwiegender öffentlicher Interessen erforderlich ist oder ein Untersuchungsverfahren gefährdet würde (Art. 24 Abs. 5 Bst. a DSG); ist die Information nicht möglich oder nur mit einem unverhältnismässig hohen Aufwand, kann ebenfalls auf eine Information verzichtet werden (Art. 24 Abs. 5 Bst. b DSG). Diese Situation liegt vor, wenn der Betroffene nicht weiss, wer alles betroffen ist oder die Anzahl Betroffener sehr gross ist.[21] Anstelle einer Information der Betroffenen sieht das Gesetz auch eine öffentliche Bekanntmachung vor (Art. 24 Abs. Bst. c DSG) vor. Diese Möglichkeit sollte jedoch nur zurückhaltend genutzt werden. Betroffene Personen können sich dabei leicht übergangen fühlen.[22]

[20] Es empfiehlt sich, Betroffene proaktiv zu informieren, auch wenn dies von Gesetzes wegen nicht unbedingt gefordert wird. Es gilt der allgemeine bekannte Grundsatz: Transparenz schafft Vertrauen. Nur in Ausnahmefällen sollte von einer Information abgesehen werden.

5. Nutzung der Daten aus dem Darknet

[21] Viele gehackte Daten finden sich im Darknet; dies heisst jedoch nicht, dass sämtliche Daten im Darknet illegale Daten sind. Bei gestohlenen Daten stellt sich die Frage, ob diese Daten legal weiterverwendet werden können.

[22] Gemäss Art. 6 Abs. 1 dürfen Daten nur rechtmässig bearbeitet werden. Bei privaten Verantwortlichen bedeutet eine nicht rechtmässige Bearbeitung ein Verstoss gegen eine strafrechtliche oder vertragsrechtliche Norm wie die unbefugte Datenbeschaffung (Art. 143 StGB) oder absichtliche Täuschung eines Vertragspartners (Art. 28f ZGB)[23, 24]. Sind Daten einmal gestohlen, bleiben diese Daten illegal.[25] Eine Verwertung solcher Daten darf nur bei schweren Verbrechen erfolgen (Art. 141 Abs. StPO). Dies wurde vom Bundesgereicht auch wiederholt im Zusammenhang mit Dashcam-Aufnahmen bestätigt.[26]

[23] Bei einer strengen datenschutzrechtlichen Auslegung müsste man also bei Daten aus dem Darknet grundsätzlich hinterfragen, ob diese Daten gestohlen sind. Kommt man zum Schluss, dass dem so ist, ist jede weitere Bearbeitung ebenfalls nicht rechtmässig.

[24] *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).

[25] Zusammengefasst bedeutet dies, 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». Braucht also ein Medienschaffender die Daten für sich, für die eigene Recherche, unterstehen diese Daten nicht dem Datenschutzgesetz. Bereits in der Botschaft zum DSG vom 19. Juni 1992 steht ausdrücklich, «Auch 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.»[27] Mit der Revision des DSG hat sich inhaltlich hier materiell nichts geändert, es ist eine rein redaktionelle Anpassung.[28]

5.1. Bankdaten

[26] Doch was, wenn die Daten Dritten übergeben, verkauft oder veröffentlicht werden sollen? Bekannt die Fälle, wo Daten von Banken oder Treuhändern gestohlen und insbesondere in Deutschland von den Steuerbehörden genutzt wurden. 2006 kauften deutsche Behörden Steuerdaten von einem ehemaligen Mitarbeiter der Liechtensteiner LGT (= Privatbank) und verurteilte die Steuerhinterziehenden;[29] 2010 wurden dann Daten von der Credit Suisse und der Bank Julius Bär gekauft[30].[31]

[27] In Deutschland hat das Bundesverfassungsgericht entschieden,[32] es gäbe keinen Rechtssatz, der festhält, «dass im Fall einer rechtsfehlerhaften Beweiserhebung die Verwertung der gewonnen Beweise stets unzulässig wäre.» Weiter vertritt das Bundverfassungsgericht folgende Auffassung: «Die Unzulässigkeit oder Rechtswidrigkeit einer Beweiserhebung führt nach Auffassung des Bundesverfassungsgerichts nicht ohne weiteres zu einem Beweisverwertungsverbot.»[33] Auch der Kassationshof in Brüssel erlaubt, dass gestohlene Daten für Justiz und Steuerbehörden genutzt werden dürfen[34].

5.1.1. Bankgeheimnis Schweiz

[28] Per 1. Juli 2015 wurde das Bankgeheimnis in Art. 47 BankG Abs. 1 um Bst. c erweitert,[35] so dass «mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft wird, wer vorsätzlich ein ihm nach Buchtstabe a offenbartes Geheimnis weiteren Personen offenbart oder für sich oder einen anderen ausnutzt.» Diese Erweiterung gilt insbesondere für Medienschaffende, wenn für diese erkennbar ist, dass die Informationen von einer Person, die unter dem Bankkundengeheimnis steht, stammen könnte.[36]

[29] Hier hat also eine Verschärfung stattgefunden; dass dies auch zu Schwierigkeiten führen kann, zeigt sich bei einer Recherche, bei welcher der Umgang der Credit Suisse mit Geldern von Kriminellen, Diktatoren etc. untersucht wurde.[37] Bei dieser Recherche konnten Schweizer Medienschaffende nicht mitwirken – internationale Medienschaffende aber schon; in der Folge wurde die Schweiz verschiedentlich kritisiert. Im Fokus standen die Pressefreiheit und der Umgang damit[38,39,40]. Es ging hier nicht um gestohlene Daten, sondern um Whistleblowing. Wobei die Person, welche die Informationen weitergab, sich ja nicht ganz gesetzeskonform verhielt, indem sie das Bankgeheimnis verletzt hatte. Also – es handelt sich wiederum um nicht rechtmässig bearbeitete Daten.

5.1.2. Datenhehlerei

[30] Einen anderen Weg hat Deutschland gewählt: Deutschland kennt 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).

[31] Die Datenhehlerei führte zu Verunsicherung bei den Medienschaffenden, weshalb die Gesellschaft für Freiheitsrecht[41] eine Verfassungsbeschwerde für diverse Medienschaffende koordinierte. Der Straftatbestand der Datenhehlerei findet gemäss Bundesverwaltungsgericht[42] keine Anwendung auf Journalistinnen und Journalisten, die mit geleakten Daten arbeiten[43].[44] Im Schweizer Gesetz findet sich kein analoger Straftatbestand, was denn auch schon zu Kritik führte.[45] Seitens der Politik wurden wiederholt Vorstösse eingereicht. Am 8. Dezember 2022 hat Ständerat Baptiste Hurni die Motion «Es ist wichtig, die Hehlerei mit digitalen Daten zu bestrafen»[46] eingereicht, nachdem im Kanton Neuenburg Daten von Patientinnen und Patienten gestohlen worden waren; der Bundesrat lehnte die Motion ab mit Hinweis auf andere Tatbestände im Strafgesetzbuch sowie das Übereinkommen des Europarates zu Cyberkriminalität. In der Folge wurde die Motion zurückgezogen. Bereits am 12. März 2013 wurde von der damaligen Nationalrätin Viola Amherd eine Motion eingereicht «Anpassung des Hehlereitatbestandes im Strafgesetzbuch»[47]; im BankG kam es dann zu einer Anpassung (vgl. Abschnitt «Bankgeheimnis»). Die Antwort des Bundesrates überzeugt und ein weiterer Tatbestand ist nicht zwingend.

5.2. Zwischenfazit

[32] Wenn gestohlene Daten genutzt werden, stellt dies einen Verstoss gegen den Grundsatz der Rechtmässigkeit von Art. 6 Abs. 1 DSG dar. Handelt es sich um Bankdaten, kommt zusätzlich Art. 47 BankG dazu.

6. Daten aus dem Darknet und Medienschaffende

[33] 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[48] publizieren regelmässig über Cyber-Vorfälle. Dabei stellt sich regelmässig die Frage: Nennung von betroffenen Personen oder Anonymisierung. Dasselbe gilt auch, wenn Whistleblower mit Medienschaffenden in Kontakt treten und Personen namentlich anschwärzen.

[34] Eine Nennung von Personennamen kann eine Persönlichkeitsverletzung im Sinne von Art. 28 ff. ZGB darstellen; dabei ist auch die sogenannte Sphärentheorie[49] zu beachten: Es ist zu differenzieren zwischen der Intim- oder Geheimsphäre (was nicht publik sein soll), der Privatsphäre (nur geteilt mit ausgewählten Personen, wie Freunden und Familie) sowie der öffentlichen Sphäre (faktisch jedermann zugänglich).[50]

[35] Medienschaffende müssen entscheiden, ob sie die Daten einzig als persönliches Arbeitshilfsmittel nutzen wollen (vgl. oben), die Daten nur in anonymisierter Form nutzen oder einen Rechtfertigungsgrund für die Veröffentlichung haben (Art 28 Abs. 2 ZGB).

[36] In den meisten Fällen entscheiden sich Medienschaffende, die Fälle anonym zu publizieren[51],[52],[53] bzw. einzig die angegriffenen Unternehmen zu nennen. Mit der Revision des DSG können sich nur noch natürliche Personen auf das Datenschutzgesetz berufen, doch bereits zuvor war es für juristische Personen nicht attraktiv, gestützt auf das Datenschutzgesetz zu klagen.

[37] Sollen Personen genannt werden, dürfte in den meisten Fällen ein überwiegendes öffentliches Interesse der Rechtfertigungsgrund sein.[54] Das Bundesgericht hat wiederholt festgehalten, dass Medien «einen Informationsauftrag» haben.[55] Bereits 1911 hat sich das Bundesgericht mit der Pressefreiheit auseinandergesetzt und die Aufgaben der Presse im Interesse eines öffentlichen Meinungsaustausches festgehalten.[56] 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[57]. In diesem Schreiben wird sie darauf hingewiesen, dass «die Bekanntgabe dieser Liste an Dritte, und damit auch an Journalisten, […] rechtswidrig» ist.[58]

7. Fazit

[39] Auch wenn es für Medienschaffende im Datenschutz gewisse Spezialnormen gibt, müssen die Grundsätze des Persönlichkeits- und Datenschutzes eingehalten werden. Die Datenschutzgrundsätze gelten selbstverständlich. Bei Daten aus dem Darknet ist insbesondere der Grundsatz der Rechtmässigkeit zu prüfen. Die weiteren Grundsätze dürften meistens keine grössere Herausforderung darstellen. Zu beurteilen bliebe allenfalls noch die Verhältnismässigkeit: dabei sollten im Sinne des «need-to-know»-Prinzips nur jene Daten bearbeitet werden, die (unbedingt) notwendig sind.

[40] Das Darknet ist eine neue Quelle für Daten und öffentlich zugänglich, wobei es dazu vertiefte Kenntnisse braucht. Gerade wenn Daten von Hacker-Gruppen angeboten werden, muss davon ausgegangen werden, dass diese nicht legal beschafft worden sind.

[41] Medienschaffende sollten, bevor sie Personen nennen, immer prüfen, ob diese Daten aus legalen oder illegalen Quellen stammen. Denn wenn die Daten illegal ins Darknet gelangt sind, ist eine Datenbearbeitung weiterhin rechtswidrig. Die Datennutzung als persönliches Arbeitshilfsmittel kann nicht verwehrt werden, für eine Publikation müsste ein überwiegendes öffentliches Interesse nachzuweisen sein. Dieses ist in jedem Fall einzeln abzuwägen und darf nicht zu schnell angenommen werden, insbesondere da heute eine Veröffentlichung auch schnell im Netz landet. Was einmal im Netz ist, kann kaum oder nur mit übermässig grossem Aufwand wieder gelöscht werden[59] bzw. kostest es viel Geld, um dies durch spezialisierte Unternehmen wie Eliminalia[60] durchführen zu lassen[61].

[42] Auch wenn Daten von Whistleblowern – ob via Darknet oder direkt – Medienschaffenden zugespielt werden, ist die Rechtmässigkeit zu prüfen. Oft handelt es sich um Geschäftsgeheimnisse, die auch nicht einfach Dritten übergeben werden dürften. Dies mussten die beiden Mitarbeiterinnen des Sozialdepartements der Stadt Zürich erfahren. Sie hatten sich im Zusammenhang mit Unregelmässigkeiten in der Sozialhilfe an die Weltwoche gewandt und wurden schlussendlich wegen Amtsgeheimnisverletzung verurteilt[62].

[43] Ein Bericht ohne Nennung der Betroffenen kann viel bewirken. Deshalb: Wenn möglich, sollte man mit Pseudonymen arbeiten und ansonsten das überwiegende öffentliche Interesse sorgfältig hinterfragen.

Exkurs: Vorfall NZZ-Mediengruppe und Umgang der Medien mit dem Datenleck

Im Rahmen der Kompromittierung der IT-Infrastruktur der NZZ-Mediengruppe im März 2023 wurden Unternehmensdaten von CH Media gestohlen und im Mai des gleichen Jahres veröffentlicht[63, 64]. Dabei handelt es sich um eine nie dagewesene Kompromittierung eines Medienhauses in der Schweiz, was naturbedingt ein hohes Interesse seitens Berufskollegen und Öffentlichkeit mit sich brachte.

Im Rahmen dieses Zwischenfalls wurden verschiedene Berichte und Interviews veröffentlicht. Die SCIP AG war eines der ersten Unternehmen, das sich mit der Veröffentlichung dieser Daten auseinandergesetzt hat.[65]

CH Media hat nach einigen Tagen mit einer superprovisorischen Verfügung versucht, einzelne Berichte und Interviews schwärzen oder entfernen zu lassen. Das Interview wurde nach einer aussergerichtlichen Einigung durch zentralplus.ch ersatzlos zurückgezogen, obwohl es inhaltlich korrekt war.[66]

Die Berichterstattung auf Inside-IT und WOZ wurden kurzfristig geschwärzt, nach einer gerichtlichen Einigung jedoch wieder freigegeben.[67]

Das Vorgehen von CH Media wurde von den Medienschaffenden breitflächig kritisiert. Die Zensur sei angestrebt worden, um die Opfer (betroffene Mitarbeiter) zu schützen, argumentierte CH Media. Diese Herleitung ist jedoch äusserst fragwürdig, da in den betroffenen Passagen keine persönlichen oder anderweitig verfänglichen Daten besprochen wurden.[68]

Stattdessen wird durch ehemalige Mitarbeiter sehr konkret das ausbleibende Informieren der Betroffenen über Geschehnisse und damit einhergehende Bedrohungen kritisiert.[69]

Darknet und der EDÖB

Dass das Darknet gerade im Hinblick auf den Datenschutz eine speziellere Rolle einnimmt, zeigt auch das Merkblatt des EDÖB gerichtet an «White Hat Hacker (WHH)»[70]. In diesem Merkblatt hält der EDÖB fest, dass jedes Hacken eine Datenbearbeitung darstellt und die Grundsätze einzuhalten sind. In seiner Schlussfolgerung hält er fest: « Alle diese Grundsätze verbieten auch die Weitergabe der durch die Sicherheitslücke betroffenen Daten oder die Bekanntgabe der Sicherheitslücke (ausser an die Aufsichtsbehörden), da sonst die betroffenen Personen geschädigt werden könnten. Eine Bekanntgabe an die Medien, bevor die Sicherheitslücke geschlossen wurde, ist daher nicht mit diesen Grundsätzen vereinbar (insbesondere, wenn der Betreiber versucht, die Sicherheitsmängel so schnell wie möglich zu beheben). Ebenso müssen die WHH den Betreiber so schnell wie möglich über ihre Feststellungen informieren und ihm ausreichend Zeit zur Behebung der Sicherheitslücken geben.»

> Kritik Martin Steiger: «Die entscheidende Frage, ob sich «ethisches Hacking» und allenfalls auch die Weitergabe an Medien mit einem überwiegenden öffentlichen Interesse gemäss Art. 31 nDSG rechtfertigen lässt, diskutiert der EDÖB nicht.»[71]

URSULA UTTINGER, lic. iur. / exec. MBA HSG, Zürich, Dozentin HSLU; www.ursula-uttinger.ch.

MARC RUEF, Gründer computec.ch, Dozent an verschiedenen Universitäten und Fachhochschulen, Mitbegründer der Firma scip AG in Zürich.

---

1 https://www.nzz.ch/technologie/kriminelle-hacker-greifen-die-nzz-an-und-erpressen-sie-cyberangriff-ransomware-ld.1778725 (Abruf 12. Juli 2024).

2 https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-100315.html (Abruf 12. Juli 2024).

3 https://www.beobachter.ch/digital/sicherheit/immer-mehr-angriffe-hacker-sturzen-sich-auf-schweizer-firmen-349877 (Abruf 12. Juli 1024).

4 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.

5 Christoph Born/Andreas Blattmann/Simon Canonica/Peter Studer, Medienrecht der Schweiz IN A NUTSHELL, 2. Auflage, Zürich/St. Gallen 2023, S. 73.

6 Martin Steiger, Kommentierung zu Art. 27 DSG, in: Thomas Steiner/Anne-Sophie Morand/Daniel Hürlimann (Hrsg.), Onlinekommentar zum Bundesgesetz über den Datenschutz – Version: 28. August 2023: https://onlinekommentar.ch/de/kommentare/dsg27 (Abruf 6. Juli 2024), N 3 ff.

7 Monika Pfaffinger, SHK-Datenschutzgesetz, Art. 31 Rz 76.

8 Rolf H. Weber, Medien im Spannungsfeld von Informationsauftrag und Datenschutz, in: Jusletter 8. Mai 2017, Rz 49.

9 Rudolf Mayer von Baldegg/Dominique Strebel, Medienrecht für die Praxis, Saldo Ratgeber, 5. Auflage, Zürich 2018, S. 10.

10 Sophia Schulze Schleithoff, Die europäische Regulierung des Datenschutzes in den Medien, 12. Dezember 2022, https://www.mdr.de/rundfunkdatenschutz/infothek/datenschutz-medien/index.html (Abruf 6. Juli 2024).

11 Rolf H. Weber (Fn. 8), Rz 2.

12 Rolf H. Weber (Fn. 8), Rz 27.

13 https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deepweb.html (Abruf 20. Juli 2024).

14 https://www.scip.ch/?labs.20160114 (Abruf 6. Juli 2024).

15 https://www.wired.co.uk/article/what-is-the-dark-web-how-to-access (Abruf 6. Juli 2024).

16 https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals (Abruf 6. Juli 2024).

17 https://www.scip.ch/?labs.20210923 (Abruf 6. Juli 2024).

18 https://www.edoeb.admin.ch/edoeb/de/home/meldeportale/databreach.html (Abruf 20. Juli 2024).

19 https://databreach.edoeb.admin.ch/report (Abruf 23. Juli 2024).

20 Ursula Uttinger/Thomas Geiser, Das neue Datenschutzrecht, Basel 2023, N 3.52.

21 Dominika Blonski, SHK DSG 2023, Art. 24 Rz 38.

22 Anlässlich eines Podiums im Januar 2024 beim MAZ wurde dies von einer vom NZZ-Hack betroffenen Journalistin geäussert.

23 Bruno Baeriswyl, SHK DSG 2013, Art. 6 Rz 13.

24 David Rosenthal, Handkommentar zum Datenschutzgesetz, Zürich 2008, aArt. 4 RZ.

25 Andrea Opel, Wider die Amtshilfe bei Datenklau: Gestohlene Daten sind gestohlene Daten, in: Jusletter 23. November 2015.

26 Urteile des Bundesgerichts 6B_1188/2018 vom 26. September 2019; 6B_810/2020 vom 14. September 2020.

27 BBl 1988 II 441.

28 BBl 2017 7012.

29 Süddeutsche Zeitung vom 15. Februar 2008 – online Ausgabe, Steuerhinterziehung: Skandal gigantischen Ausmasses.

30 BZ (= Berner Zeitung) vom 18. Oktober 2010, Erneut Steuer CD von der Schweiz verkauft.

31 https://de.wikipedia.org/wiki/Steuers%C3%BCnder-CD (Abruf 27. Juli 2024).

32 Beschluss des Bundesverfassungsgerichts vom 9. November 2010 (2 BvR 2101/09).

33 https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-109.html (Abruf 23. Juli 2024).

34 https://www.vrt.be/vrtnws/de/2017/03/07/justiz_darf_gestohlenebankdatennutzen-1-2910688/ (Abruf 23. Juli 2024).

35 BBl 2014 6236 f.

36 Born/Blattmann/Canonica/Studer (Fn. 5), S. 137 f.

37 https://www.occrp.org/en/suisse-secrets/ (Abruf 27. Juli 2024).

38 https://www.tagesanzeiger.ch/weltweite-kritik-am-umgang-der-schweiz-mit-der-pressefreiheit-884403267706 (Abruf 20. Juli 2024).

39 https://www.nzz.ch/schweiz/bankgeheimnis-contra-pressefreiheit-ld.1712246 (Abruf 20. Juli 2024).

40 https://www.tagesanzeiger.ch/bundesanwaltschaft-ermittelt-wegen-datendiebstahl-bei-der-credit-suisse-153274552072 (Abruf 20. Juli 2024).

41 https://freiheitsrechte.org/ (Abruf 25. Juli 2024).

42 Bundesverfassungsgericht (1 BvR 2821/16).

43 https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-datenhehlerei-bverfg (Abruf 23. Juli 2024).

44 https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/verfassungsgericht-staerkt-pressefreiheit (Abruf 23. Juli 2024).

45 Blog von Michèle Trebo: Datenhehlerei – Lücke im Schweizerischen Strafgesetz? Vom 9. Juni 2022, https://www.scip.ch/?labs.20220609 (Abruf 25. Juli 2024).

46 Motion 22.4325 «Es ist wichtig, die Hehlerei mit digitalen Daten zu bestrafen», eingereicht von Baptiste Hurni.

47 Motion 12.3123 «Anpassung des Hehlereitatbestandes im Strafgesetzbuch», eingereicht von Viola Amherd.

48 Otto Hostettler, 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».

49 BGE 118 IV 45 ff. oder auch BGE 140 III 28 ff.

50 Mayer von Baldegg/Strebel (Fn. 9), S. 170.

51 Otto Hostettler, Hacker stürzen sich auf Schweizer Firmen, Beobachter, veröffentlicht am 6. Oktober 2021, https://www.beobachter.ch/digital/sicherheit/immer-mehr-angriffe-hacker-sturzen-sich-auf-schweizer-firmen-349877 (Abruf 28. Juli 2024).

52 Otto Hostettler, Jetzt wird's richtig gefährlich, Beobachter, veröffentlicht am 12. Mai 2022, https://www.beobachter.ch/multimedia/digital/jetzt-wirds-richtig-gefahrlich-379199 (Abruf 28. Juli 2024).

53 Otto Hostettler, Hacker erpressen Bernina und fordern 1.3 Millionen, Beobachter, veröffentlicht am 28. April 2023, https://www.beobachter.ch/digital/cybercrime-ransomeware-banden-erpressen-nahmaschienhersteller-bernina-und-fordern-losegeld-597553 (Abruf 28. Juli 2024).

54 Born/Blattmann/Canonica/Studer (Fn. 5), S. 29.

55 BGE 122 III 449 E. 3b.

56 BGE 37 I 381.

57 https://www.zentralplus.ch/technologie-digitales/luzerner-hackerin-veroeffentlicht-flugverbotsliste-der-usa-2513319/ (Abruf 1. August 2024).

58 Schreiben des EDÖB an Maia Arson Kottmann vom 7. Februar 2023, S. 2.

59 Urteil des deutschen Bundesgerichtshofs Az. VI ZR 476/18 vom 23. Mai 2023.

60 https://eliminalia.com/ch/ (Abruf 2. August 2024).

61 https://www.nzz.ch/feuilleton/diese-firma-loescht-die-wahrheit-ld.1726792 (Abruf 2. August 2024).

62 https://www.sozialinfo.ch/fachinformationen/sozialpolitik-2003-2018/monika-stocker-und-die-whistleblowerinnen (Abruf 2. August 2024).

63 https://chmedia.ch/news/daten-von-ch-media-nach-cyberangriff-veroeffentlicht (Abruf 6. Juli 2024).

64 https://chmedia.ch/news/cyberkriminelle-veroeffentlichen-erneut-daten-von-ch-media (Abruf 6. Juli 2024).

65 https://twitter.com/mruef/status/1653661089370976256 (Abruf 6. Juli 2024). Unter anderem ist von Marc Ruef, Head of Research bei SCIP AG, ein Interview auf zentralplus.ch publiziert worden.

66 https://www.zentralplus.ch/in-eigener-sache/zentralplus-und-ch-media-einigen-sich-aussergerichtlich-2555117 (Abruf 6. Juli 2024).

67 https://www.inside-it.ch/hausmitteilung-inside-it-und-woz-duerfen-zensierte-passagen-wieder-aufschalten-20230619, https://www.woz.ch/2319/!103XWAKDKV88 (Abruf 6. Juli 2024).

68 https://www.woz.ch/2318/!1MKWN85ZSV5C (Abruf 6. Juli 2024).

69 https://www.republik.ch/2023/07/04/die-stille-nach-dem-datenklau (Abruf 1. Juli 2024).

70 EDÖB, Merkblatt White Hat Hacker/innen (WHH): Ihre rechtliche Situation, ihre Risiken und die Rolle des EDÖB vom 27. Juni 2023.

71 https://steigerlegal.ch/2023/06/27/white-hat-hacker-merkblatt-edoeb/ (Abruf 28. Juli 2024).