LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

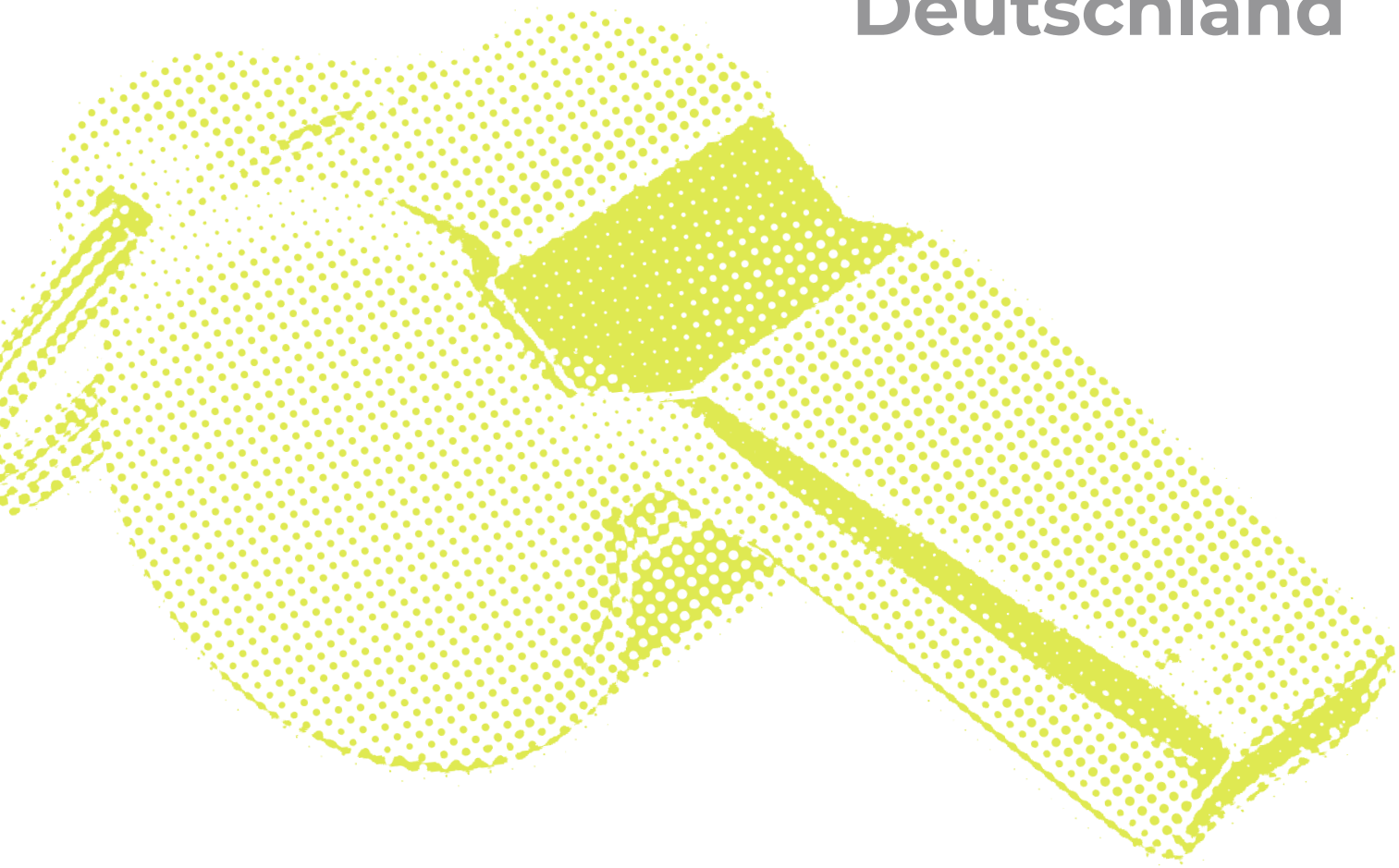
Vigilanz Kulturen
SFB 1369

Working Paper

www.sfb1369.uni-muenchen.de

01/2020

Zur anstehenden Regulierung von Whistleblowing in Deutschland



Inhalt

SFB Vigilanzkulturen – Working Papers

Die Working Papers werden vom Sonderforschungsbereich 1369 Vigilanzkulturen. Transformationen – Räume – Techniken herausgegeben und sind auf der Website des SFB sowie auf der Open Access-Plattform der LMU München abrufbar.

Mit Zusendung des Typoskripts überträgt die Autorin/der Autor dem Sonderforschungsbereich ein nichtexklusives Nutzungsrecht zur dauerhaften Hinterlegung des Dokuments auf der Homepage des SFB 1369 sowie dem Dokumentenserver der LMU. Das Urheberrecht verbleibt bei den AutorInnen. Die Einhaltung von eventuellen Sperrfristen sowie von Urheber- und Verwertungsrechten Dritter obliegt den AutorInnen.

Die Veröffentlichung eines Beitrages als Preprint in den Working Papers ist kein Ausschlussgrund für eine anschließende Publikation in einem anderen Format.

Diese Publikation wurde gefördert von der Deutschen Forschungsgemeinschaft

DOI: https://doi.org/10.5282/ubm/epub.70684
Online-ISSN: 2699-9242

URL: https://www.sfb1369.uni-muenchen.de/forschung/publikationen/working-papers/index.html

Sonderforschungsbereich 1369 Vigilanzkulturen. Transformationen – Räume – Techniken
Ludwig-Maximilians-Universität München
Geschwister-Scholl-Platz 1
80539 München

www.sfb1369.lmu.de
m.heger@lmu.de

Gestaltung: Sofarobotnik

Ralf Kölbel

Vorbemerkung

Es gehört zu den Kennzeichen des Sonderforschungsbereichs 1369 „Vigilanzkulturen“, die in seinem Titel bezeichneten Phänomene in einem weiten Bogen und einer außerordentlichen historischen Vielfalt in den Blick zu nehmen. Darin eingeschlossen sind ausgesprochen heutige Spielarten von Vigilanz. Dies wiederum kann zur Notwendigkeit führen, von aktuellen Entwicklungen nicht nur Notiz zu nehmen, sondern hierauf auch zu reagieren. Für die Problematik des Whistleblowings, die in einem der Teilprojekte des SFB bearbeitet wird, entstand dieser Bedarf durch das Wirksamwerden der Europäischen Richtlinie 2019/1937 (EU) des Europäischen Parlaments und des Rates vom 23. Oktober 2019. Dadurch kann sich die hiesige Rechtspolitik den durchaus vielgestaltigen Problemen, die sich beim Whistleblowing und dessen Rahmensetzung ergeben, nämlich nicht länger entziehen. War es ihr bislang möglich, sich einer rechtlichen Ausgestaltung der Problematik (trotz mehrfacher Gesetzesinitiativen) immer wieder zu enthalten, steht sie dank des Europäischen Rechts nunmehr für eine dezidierte Festlegung ausdrücklich in der Pflicht. Dies war Anlass für einen größeren SFB-Workshop, der am 15.11.2019 stattfand. Hier wurde einigen Fragen nachgegangen, die für die bevorstehende deutsche Whistleblowing-Legislatur maßgeblich sind – die empirischen Bedingungen des Gegenstands, die derzeitigen Regelungsdefizite und die nunmehrigen Neuregelungsoptionen. Die Vorträge und die diskussionseinleitenden Statements sind in diesem Working Paper dokumentiert.

Vortrag zur Veranstaltung

Prof. Dr. Ralf Kölbel / Dr. Nico Herold, LMU München

Whistleblowing in der empirischen Forschung

I. Einleitung

Die Frage nach einem gesetzlichen Rahmen für Whistleblowing in Deutschland ist (abermals) virulent geworden. Nach dem Scheitern aller bisherigen rechtspolitischen Vorstöße und Gesetzesentwürfe hat der Erlass der Whistleblowing-Richtlinie (EU) 2019/1937 (im Folgenden: WB-RL) zu einer legislatorischen Inpflichtnahme geführt. Innerhalb der nächsten Jahre wird es eine neue dezidierte Regelung geben müssen, bei deren Ausgestaltung es diverse Vorgaben der WB-RL umzusetzen, aber auch manche Gestaltungsspielräume auszufüllen gilt. Insofern ist mit einer Belebung der dahingehenden rechtspolitischen Debatte zu rechnen. Deren Gehalt dürfte profitieren, wenn sie sich nicht nur auf der Ebene des Dafürhaltens und der politischen Reflexion bewegen muss, sondern die empirischen Gegebenheiten des Gegenstandes berücksichtigen kann. Daher soll im Folgenden ein Überblick über den Stand der einschlägigen Forschung gegeben werden.

Dies setzt zunächst eine knappe Verständigung darüber voraus, was in diesem Beitrag mit Whistleblowing gemeint ist. Die internationale empirische Literatur operiert hier mit einem weiten Begriff und assoziiert Whistleblowing mit „the disclosure by organization members (former or current) of illegal, immoral or illegitimate practices under the control of their employers, to persons or organizations that may be able to effect action".[1] Kennzeichnend ist also, dass sich ein "Insider"[2] einer Organisation (sei es nun ein Unternehmen, eine Behörde, ein Geheimdienst, die Streitkräfte, eine Universität o.ä.) im Wissen um einen organisationsinternen Missstand glaubt und diese Kenntnisse sodann weitergibt. Geschieht dies innerhalb der Organisation – etwa gegenüber der Behörden-/Unternehmensleitung oder einer speziellen Whistleblowing-Stelle (einschließlich Ombudspersonen) – handelt es sich um internes Whistleblowing.[3] Wenden sich die Hinweisgeber dagegen an Kontroll- und Strafverfolgungsbehörden oder gar an die Medien, spricht man allgemein von externem Whistleblowing. Die WB-RL knüpft hieran an, unterscheidet bei der externen Variante aber zwischen „externen Meldungen" an die zuständigen Behörden (Art. 5 Nr. 5) und der „Offenlegung" als dem „öffentlichen Zugänglichmachen von Informationen" (Art. 5 Nr. 6).

II. Wie oft kommt Whistleblowing vor?

Was die praktische Relevanz dieser verschiedenen Spielarten betrifft, ist eine Differenzierung angezeigt: Die besten Hinweise zur Frage nach der Prävalenz von Whistleblowing ergeben sich aus Befragungen von Unternehmens- und Behördenmitarbeitern. Diese sollen dabei Auskunft darüber geben, ob sie schon einmal Kenntnis von Missständen in ihren Organisationen erlangt und wie sie sich bejahendenfalls in dieser Situation verhalten haben. Den so erhobenen Angaben zufolge nimmt – bei einer erheblichen Bandbreite der internationalen Einzelergebnisse – ungefähr jeder zweite Insider eine Meldung vor,[4] dies aber offenbar mehrheitlich (zunächst auf dem normalen Dienstweg) an Verantwortliche, Vorgesetzte oder Kollegen.[5] Besonders selten ist externes Whistleblowing. Nach den meisten hierzu vorliegenden internationalen Studien geben (deutlich) unter 10 % der Insider ihr Wissen (direkt) nach außen.[6] Insgesamt muss man also davon ausgehen, dass erstens bei einem ganz erheblichen Anteil wahrgenommener Missstände letztlich Stillschweigen gewahrt wird und dass zweitens jene Personen, die die Dinge ansprechen, ganz klar die interne Klärung bevorzugen. Externes Whistleblowing ist dagegen ein atypisches Verhalten. Es zeigt sich über alle Studien hinweg, dass Whistleblower in aller Regel nur dann nach außen gehen, wenn sie intern (nach ggf. wiederholten Versuchen) erfolglos geblieben sind.[7] Fast nie wenden sie sich ohne einen internen Abhilfeversuch gleich im ersten Schritt an die Strafverfolgungsbehörden oder die Medien.[8]

III. Was führt zu Whistleblowing und wie wird man zum Whistleblower?

1. Relevante Faktoren

Das wirft die Frage auf, unter welchen Bedingungen es zu diesen Ausnahmen kommt. Die internationale Whistleblowing-Forschung untersucht auch dieses Problem vorwiegend mit diversen Befragungsverfahren, wobei man sich auf eine Reihe von personalen und situativen Faktoren konzentriert (zu den ebenfalls vertieften organisatorischen Faktoren siehe unten V.2.). Diesen Studien zufolge hat die Persönlichkeit der Insider auf die Entscheidung, das fragliche Wissen überhaupt (und an wen) weiterzugeben, den geringsten Einfluss. Zwar finden manche Untersuchungen durchaus gewisse Unterschiede zwischen der schweigenden Gruppe und jenen Personen, die sich an interne Stellen oder auch an externe Institutionen wenden. Das betrifft neben allgemeinen Wertehaltungen oder der Akzeptanz von Whistleblowing ganz verschiedene Merkmale (z.B. persönliche Autonomie, Dauer der Betriebszugehörigkeit, innerorganisatorische Stellung, Verbundenheitsgefühl). Doch insgesamt sind die hierzu vorliegenden Studienergebnisse uneinheitlich und zuweilen widersprüchlich.[9] Offenbar gibt es keinen steckbrieftauglichen Typus der Whistleblower-Person. Vielmehr kann grundsätzlich jede/r in eine Situation geraten, in der er/sie sukzessive zum/r Hinweisgeber/in wird. Besser gesichert und klarer ist dagegen die Whistleblowing-Relevanz einiger situativer Gegebenheiten und Verläufe. Der Hauptfaktor, der Insider zu einer ersten Meldung bringt, liegt danach sehr wahrscheinlich in der Art und dem Ausmaß des wahrgenommenen Missstandes.[10] Außerdem spielt etwa die individuell eingeschätzte Qualität der Beweislage eine Rolle.[11] Hemmend wirken vor allem die Angst vor persönlichen negativen Konsequenzen (z.B. rechtliche Verfolgung, finanzielle Nachteile, Reputationsschäden) und die mangelnde Aussicht auf den Meldungserfolg.[12]

Allerdings handelt es sich bei den meisten Arbeiten, die diesen Befunden zugrunde liegen, um sog. Laborstudien.[13] Üblicherweise werden hier gewisse Gruppen von Studierenden oder Unternehmensbeschäftigten zusammengestellt, denen man kurze, fiktive Fallschilderungen bzw. Geschichten vorlegt und sie nach ihrem Verhalten in der jeweils beschriebenen Situation fragt. Die hierauf gegebenen Antworten werden dann auf statistische Zusammenhänge mit bspw. persönlichen Eigenschaften oder systematisch variierten Fallmerkmalen hin untersucht. Erhoben werden dabei aber im Grunde nur die Bedingungen von Handlungsabsichten, nicht aber die des Handelns selbst. Ob die befragten Personen jemals in eine der geschilderten Situationen kommen und dann tatsächlich in der von ihnen angegebenen Weise handeln werden, ist völlig unklar.[14] Fraglich bleibt auch, inwiefern die meist sehr kleinen Untersuchungsgruppen überhaupt repräsentativ für die Bevölkerung sind.[15] Deshalb ist die Tragweite der besagten Forschungslinie letztlich begrenzt.

1 *Taylor,* Public Administration Review 78/5 (2018), S. 718; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 120; *Miceli/Near,* Australian Journal of Public Administration 72/4 (2013), S. 435 f.; grundlegend *Near/Miceli*, Journal of Business Ethics 4/1 (1985), S. 4.
2 Typischerweise beruht der Insider-Status auf der Organisationsmitgliedschaft, etwa als (ehemalige/r) Mitarbeiter/in. Denkbar sind aber auch gelockerte Formen der Organisationsmitgliedschaft (Lieferanten- oder Kundenbeziehung usw.). Vgl. auch *Schmolke*, ZGR 48/5 (2019), S. 880 f. Die WB-RL legt einen sehr weiten persönlichen Anwendungsbereich an, der gem. Art. 4 Abs. 4 b) sogar „Dritte, die mit den Hinweisgebern in Verbindung stehen und in einem beruflichen Kontext Repressalien erleiden könnten, wie z.B. Kollegen oder Verwandte des Hinweisgebers" erfasst.
3 Kein echtes internes Whistleblowing liegt vor, wenn die Meldung auf dem regulären Dienstweg, etwa gegenüber direkt Vorgesetzten, erfolgt. Siehe dazu etwa *Herold*, Whistleblower, 2016, S. 40 f., 46; vgl. auch *Schmolke,* ZGR 48/5 (2019), S. 882; *Miceli/Near,* Australian Journal of Public Administration 72/4 (2013), S. 435.
4 *Olsen*, in: *Brown et al.* (Hrsg.) International Handbook on Whistleblowing Research, 2014, S. 178 ff., 184, 204. In 3 von 5 großen norwegischen Untersuchungen meldeten zwischen 53 % und 55 % der Arbeitnehmer verschiedenster Felder. Siehe dazu *Trygstad/Ødegård/Svarstad,* in*: Lewis/Vandekerckhove* (Hrsg.), Selected papers from the International Whistleblowing Research Network conference, 2017, S. 28 ff.; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 120, 129. Für ähnliche Befunde siehe auch *Taylor,* Public Administration Review 78/5 (2018), S. 719 f.; *Ethics & Compliance Initiative* (Hrsg.), Global Business Ethics Survey. Measuring Risk and Promoting Workplace Integrity, 2016, S. 8.
5 Entsprechende Daten bei *Graaf*, International Public Management Journal 22/2 (2019), S. 220 ff.; *Ethics Resource Center* (Hrsg.), National Business Ethics Survey of the U.S. Workforce, 2014, S. 30; *dies.* (Hrsg.), Inside the Mind of a Whistleblower, 2012, S. 11 f.; *Public Concern at Work* (Hrsg.), Whistleblowing: the inside story, 2013, S. 13. Beispielsweise erfolgten bei *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 130 nur 17 % aller erhobenen Meldungen über das interne Whistleblowing-System.
6 Für eine Zusammenfassung diesbzgl. Befunde siehe *Lewis/Brown/Moberly*, in: *Brown et al.* (Hrsg.) International Handbook on Whistleblowing Research, 2014, S. 20; siehe auch die Studien bei *Kölbel/Herold*, Deviant Behavior 40/2 (2019), S. 6; *Herold*, Whistleblower, 2016, S. 349.
7 *Vandekerckhove/Phillips*, Journal of Business Ethics 159/1 (2019), S. 209. Auch größere Surveys gelangen zu diesem Befund, vgl. etwa *Miceli/Near*, Australian Journal of Public Administration 72/4 (2013), S. 438, 443 f.; *Public Concern at Work* (Hrsg.), Whistleblowing: the inside story, 2013, S. 4, 12 f.; an der "Kontraindiziertheit" externen Whistleblowings ändern im Übrigen auch finanzielle Anreize wenig, siehe dazu z.B. *U.S. Securities and Exchange Commission, Whistleblower Program*. 2019 Annual Report to Congress, S. 18; *National Whistleblowers Center*, Impact of Qui Tam Laws on Internal Corporate Compliance, 2010, S. 5 f.; *Kesselheim/Studdert/Mello*, New England Journal of Medicine 362/19 (2010), S. 1834.
8 Siehe z.B. *Public Concern at Work* (Hrsg.), Whistleblowing: the inside story, 2013, S. 13; *Donkin/Smith/Brown,* in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 86 ff.
9 Siehe die Übersichtsarbeiten bei *Lee/Xiao*, Journal of Accounting Literature 41 (2018), S. 32 ff.; *Gao/Brink*, Journal of Accounting Literature 38 (2017), S. 4; *Herold*, Whistleblower, 2016, S. 94 f., 210 ff., 316 jeweils m.w.N.
10 Übersicht bei *Lee/Xiao*, Journal of Accounting Literature 41 (2018), S. 38; *Gao/Brink*, Journal of Accounting Literature 38 (2017), S. 8; *Herold*, Whistleblower, 2016, S. 357 f.; siehe auch *Taylor/Curtis*, Behavioral Research in Accounting, 25/2 (2013), S. 32.
11 *Ethics & Compliance Initiative* (Hrsg.), Global Business Ethics Survey. Measuring Risk and Promoting Workplace Integrity, 2016, S. 19; *Brink/Lowe/Victoravich*, Auditing: A Journal of Practice & Theory 32/3 (2013), S. 97 f.; *Dworkin/Baucus*, Journal of Business Ethics 17/12 (1998), S. 1296.
12 EU-Kommission, Summary results of the public consultation on whistleblower protection, 2018, S. 6; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 129 f.; *Guthrie/Taylor*, Journal of Forensic Accounting Research 2/1 (2017), S. A8 ff.; *Bussmann/Niemeczek/Vockrodt*, MschrKrim 99/5 (2016), S. 32 f.; *Gold/Walden/Devine*, Why Whistleblowers Wait, 2016, S. 9 ff.; *Ethics & Compliance Initiative* (Hrsg.), Global Business Ethics Survey. Measuring Risk and Promoting Workplace Integrity, 2016, S. 8; *Gao/Greenberg/Wong-On-Wing*, Journal of Business Ethics 126/1 (2015), S. 95; *Firth-Cozens/Firth/Booth*, Clinical Governance: An International Journal 8/3 (2003), S. 333 f.
13 Kennzeichnend z.B. *Mechtenberg/Muehlheusser/Roider*, Whistleblower Protection: Theory and Experimental Evidence, 2018, S. 8.
14 Siehe dazu grundlegend *Mesmer-Magnus/Viswesvaran*, Journal of Business Ethics 62/3 (2005), S. 278 ff.; auch *Gao/Greenberg/Wong-On-Wing*, Journal of Business Ethics 126/1 (2015), S. 97.
15 *Olsen*, in: *Brown et al.* (Hrsg.), International Handbook on Whistleblowing Research, 2014, S. 199 f.

2. Eigene Verlaufsstudie

Vorzuziehen sind folglich Untersuchungen, die echte Fälle von Hinweisgebern analysieren. Da es aber schwierig ist, solche Personen zu erreichen, sind derartige Studien selten. Eine der wenigen Ausnahmen haben wir im Rahmen eines DFG-Forschungsprojektes durchgeführt.[16] Die Arbeit beruhte im Kern auf Interviews mit 28 Whistleblowern ganz verschiedener Bereiche (Gesundheitswesen, öffentlicher Dienst, Unternehmen), aus deren Analyse sich ein typischer Verlaufsprozess ergab, der sich mit den Ergebnissen ähnlich gelagerter internationaler Studien weitgehend deckt.[17]

a) Der typische Whistleblowing-Prozess

Demnach ist externes Whistleblowing charakteristischerweise das Ergebnis einer innerorganisatorischen Eskalation. Nach der Wahrnehmung des Missstands wird dieser durch den Insider meist informell thematisiert, also bspw. bei beteiligten Personen oder Vorgesetzten angesprochen.[18] Sofern das nicht zu dem erwünschten Ergebnis führt, erfolgt in der Regel eine Meldung an die Organisationsführung oder eine andere Stelle, nicht selten auch wiederholt. Wenn sich in der weiteren Folge dann auch der Gang an die Strafverfolgungs- und/oder Kontrollbehörden anschließt, so geschieht das indes meist nur im Zuge eines wechselseitigen Aufschaukelns. Dieses basiert teilweise darauf, dass die Mitteilungsempfänger anders reagieren, als es vom Whistleblower beabsichtigt ist, indem sie den Missstand z.B. verleugnen, verharmlosen oder nur vordergründig abstellen. In anderen Fällen greift die Organisation bzw. die verantwortliche Person sogar zu mehr oder minder verdeckten Repressalien, um den Whistleblower von (weiteren) Handlungen abzubringen (besonders wenn dieser bisher eine gewisse Beharrlichkeit zeigt).

Die hierdurch ausgelöste Eskalationsdynamik setzt in der Regel zunächst mit einer Verschlechterung des persönlichen Verhältnisses zu den Verantwortlichen ein. Bis dahin strebt der Insider nahezu immer eine schnelle, aufwandsarme und geräuschlose Missstandsbehebung an, ohne Strafverfolgungsbehörden oder Medien einschalten zu wollen. Fühlt er sich aber in seinen Bemühungen hingehalten oder zurückgewiesen, weil sein Vorbringen nicht aufgegriffen oder gar abgewehrt wird, bleibt sein Handlungsimpuls hoch. Manchmal hat er das Gefühl, in seiner Integrität oder seiner Kompetenz in Frage gestellt zu werden. Er gerät so zusehends unter Zugzwang, intern weiter gegen den Missstand vorzugehen. Lenkt er deswegen nicht ein (etwa auch aus dem Gefühl, im Recht zu sein), wird er zu einem „Störfaktor“ für die jeweiligen Verantwortlichen und/oder die Organisation. Dies löst (weitere) Gegenmaßnahmen aus, die sich in Schwere und Art schrittweise steigern – und für die Betroffenen schließlich als ein eigener, neuer Missstand in den Vordergrund rücken. Da die Behandlung der Hinweisgeber oft sensible persönliche Bereiche berührt (Karriere, Gesundheit, persönliche Integrität etc.),[19] überlagert sie vielfach das ursprünglich angezeigte Problem und wird oft zu dem eigentlichen Grund, um schließlich nach außen zu gehen. So gesehen stellt sich externes Whistleblowing oft ganz und gar nicht als ein nur-ethisch motiviertes Verhalten dar. Stattdessen ist es beinahe immer ein Anzeichen dafür, dass die organisationsinternen Mechanismen im Umgang mit Missständen und Hinweisen schlecht funktionieren[20] – was die Hinweisgeber dazu bringt, mit der externen Informationsweitergabe auch eigene Interessen zu verfolgen.[21]

b) Verlaufsbeeinflussende Bedingungen

Für die subjektiv empfundene Dringlichkeit, mit der sich Insider zu Offenlegungshandlungen veranlasst sehen, ist zunächst der jeweilige Missstand maßgeblich. Eine Handlungsnotwendigkeit wird vor allem bei solchen gesehen, die Individualrechtsgüter betreffen (etwa: drohende gesundheitliche, und nicht allein finanziellen Schäden). Besonders bedeutsam für die Handlungsmotivation ist zudem, ob sich die Insider persönlich durch den Missstand gefährdet sehen.[22] Zugleich variieren sie aber darin, wie ansprechbar sie für solche Anstöße sind und in welchem Maße sie sich von nachteiligen Mitteilungsfolgen abschrecken lassen. Nicht wenige Personen stecken in den fraglichen Situationen eher zurück und vermeiden die Eskalation, etwa wenn sie generell eher konfliktscheu veranlagt sind. Andere Menschen zeigen eine offensivere Tendenz, insbesondere bei als moralisch besonders gewichtig eingestuften oder individuell relevanten Problemlagen. Das gilt gerade auch dann, wenn sie sich in einer Weise behandelt fühlen, die in ihnen Wut, Empörung oder Vergeltungsbedürfnisse weckt. Daneben haben wir aber auch noch einen anderen Typus gefunden. So kann bei Personen, die Missstände eher nüchtern betrachten und ihre Handlungsmöglichkeiten und Erfolgsaussichten vernünftig abwägen, ein zentraler Antrieb für die Mitteilungsbereitschaft auch (besonders später im Verlauf) in einem Selbstschutz- oder Rehabilitierungsbedürfnis liegen. Wichtig bei all dem ist, dass die Organisationsgegebenheiten den Rahmen für die Möglichkeiten setzen, eine Meldung ins Leere laufen zu lassen, einen Whistleblower zu maßregeln und so die eben angesprochene Eskalation auszulösen. Bei Organisationen mit einer starken inneren Hierarchie nehmen bspw. mit der Ranghöhe allgemein auch die Möglichkeiten zur Vertuschung und Vergeltung eindeutig zu. Relevant ist in diesem Zusammenhang auch das konkrete Hierarchieverhältnis zwischen Insider und Verantwortlichen.[23]

16 Siehe für das Folgende ausführlich *Herold*, Whistleblower, 2016, S. 158 ff., 313 ff. und zusammenfassend *Kölbel/Herold*, Deviant Behavior 40/2 (2019), S. 133 ff.; *dies.* NK 16/4 (2015), S. 375 ff.
17 Vgl. etwa *Vandekerckhove/Phillips*, Journal of Business Ethics 159/1 (2019), S. 201 ff.; *Hedin/Månsson*, European Journal of Social Work 15/2 (2012), S. 151 ff.
18 Siehe zu diesem Verhalten z.B. auch *Bussmann/Niemeczek/Vockrodt*, MschrKrim 99/5 (2016), S. 32; *Ethics Resource Center* (Hrsg.), National Business Ethics Survey of the U.S. Workforce, 2014, S. 30; *Donkin/Smith/Brown*, in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 88.
19 Dies betrifft spiegelbildlich allerdings auch die vom Whistleblowing betroffenen Organisationsmitglieder. Deren Karriere ist ebenfalls gefährdet, besonders im Zuge eines „stigma managements“ ihrer Organisation, die die Verantwortung für strukturelle Missstände häufig als Einzelfall- und/oder Individualprobleme ausflaggt und einzelnen Personen zuschreibt (dazu etwa *Warren*, Business Ethics Quarterly 17/3 (2007), S. 483 ff.).
20 Vgl. z.B. auch *Donkin/Smith/Brown*, in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 92.
21 Bei den in der Erhebung interviewten Whistleblowern lag im Übrigen auch schon zu Beginn des Prozesses nicht nur eine altruistische Motivlage vor. Es spielten immer auch persönliche Belange eine Rolle (etwa die eigene Betroffenheit vom oder Involvierung in den Missstand).
22 Beispiele bei *Herold*, Whistleblower, 2016, S. 205, 224 f, 326.
23 Beispiele bei *Herold*, Whistleblower, 2016, S. 280 ff.; siehe dazu auch *Taylor/Curtis*, Behavioral Research in Accounting 25/2 (2013), S. 30 ff.

IV. Die öffentliche Wahrnehmung von Whistleblowing

Eine weitere empirische Frage betrifft den Umgang mit Whistleblowing, sowohl im sozialen Umfeld der Whistleblower, als auch in der generellen öffentlichen Bewertung des Phänomens. So ist anzunehmen, dass in einem Gemeinwesen, das Whistleblowing prinzipiell wertschätzt, Insider vermutlich eher zur Informationsweitergabe neigen und auch bessere Mitteilungswege vorfinden, als dies in einer Gesellschaft zu erwarten ist, die Whistleblowing ablehnt.[24] Dort muss der Insider auch eher mit zurückweisenden Reaktionen seiner beruflichen und privaten Umgebung rechnen, was ihn schwerlich ermutigen wird. Das könnte erklären, warum die Häufigkeit von Whistleblowing in jenen Ländern und Kulturen höher ist, in denen sich die Bevölkerung in Befragungen vergleichsweise positiv zu Whistleblowing äußert, was tendenziell eher für westliche, individualistisch geprägte Gesellschaften gilt, allen voran die USA.[25]

In der wissenschaftlichen Literatur wird allerdings vermutet, dass die jeweiligen Einstellungen innerhalb einzelner Gesellschaften in dieser Frage keineswegs eindeutig sind. Jedenfalls werden Hinweisgeber nicht selten als illoyal empfunden und abgelehnt, was man daran erkennen kann, dass sie immer wieder soziale Zurückweisung erleben. Personen, die einen Missstand organisationsintern oder -extern gemeldet haben, berichten häufig (wenn auch nicht immer) davon, anschließend von ihren Kollegen/-innen informell sanktioniert worden zu sein.[26] Eine Befragung unter 1.000 deutschen Arbeitnehmern ergab z.B., dass Hinweisgeber zu 55 % (privater Sektor) bzw. 17 % (öffentlicher Sektor) Opfer von Vergeltungsmaßnahmen wurden.[27] International variieren die dahingehenden Raten allerdings stark,[28] wobei die Vergeltungswahrscheinlichkeit mit der Anzahl der Mitteilungsversuche[29] und der Wahl externer Adressaten[30] zuzunehmen scheint.

Gerade im beruflichen Umfeld, d.h. unter den Kollegen/-innen von Hinweisgebern, besteht also offenbar häufig das Gefühl, dass die Mitteilung eines Missstands dem Unternehmen oder der Organisation schadet und deshalb Solidaritätsnormen verletzt. Hierin liegt, das muss man klar konstatieren, auch eine Wirkungsgrenze des Rechts. Mögen alle Arten von Repressionen, etwa das Mobbing von Hinweisgebern, deren Ausgrenzung, Diskriminierung und eine benachteiligende oder ungleiche Behandlung usw. auch verboten und sanktioniert sein (dazu jetzt etwa Art. 19 ff. WB-RL). Dass ein Hinweisgeber innerhalb seines Umfeldes isoliert wird oder die Zurückweisung der Kollegen erfährt, lässt sich mit rechtlichen Mitteln aber schwerlich (ganz) verhindern.[31]

Deswegen ist es umso mehr von Belang, dass bzw. ob Whistleblowing sozial akzeptiert wird. Vermutlich hängt dies jedoch von zahlreichen Aspekten des Einzelfalls ab (um welche Missstände geht es? schreibt man dem Hinweisgeber selbstsüchtige Absichten zu? wie ist er oder sie vorgegangen? wo wurde das Wissen enthüllt?). Die wenigen hierzu vorliegenden Befunde weisen nämlich recht klar darauf hin, dass das öffentliche Bild des Hinweisgebers zwischen dem des Helden und dem des Verräters changieren kann. Hierfür aufschlussreich sind Studien, die den Tenor der medialen Berichterstattung systematisch ausgewertet haben. Sie zeigen auf, wie konkrete Whistleblowing-Fälle (oder Whistleblowing allgemein) in der Presse aufbereitet und präsentiert worden sind. Solche Untersuchungen liegen nicht nur international[32], sondern auch für den deutschsprachigen Bereich vor[33]. Dort wurden bspw. verschiedene Leitmotive ausgemacht, die die Grundausrichtung des jeweiligen Textes prägten. Danach hatten 42 % der ausgewerteten Pressebeiträge die Hinweisgeber als Personen dargestellt, die Zivilcourage zeigen, d.h. der Öffentlichkeit einen Dienst erweisen und dabei erhebliche Nachteile in Kauf nehmen. In der Regel wird diese positive Perspektive aber keineswegs durchgehend geteilt. Mit Blick auf dieselben Fälle haben 31 % der Veröffentlichungen die Whistleblower als eigennützige Personen angesehen, die sich in erster Linie bereichern oder profilieren wollen.[34]

24 So auch *Schmolke*, ZGR 48/5 (2019), S. 882 ff.
25 Zur kulturellen Dimension und der im Detail uneindeutigen Erkenntnislage zusammenfassend *Vandekerckhove*, in: *Brown et al.* (Hrsg.) International Handbook on Whistleblowing Research, 2014, S. 37 ff.; *Herold*, Whistleblower, 2016, S. 89 ff., jeweils m.w.N.
26 *Park/Bjørkelo/Blenkinsopp*, Journal of Business Ethics 23/4 (2018); *Smith/Brown*, in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 122 ff.; Übersichten bei *Herold*, Whistleblower, 2016, S. 105 ff.; *Smith*, in: *Brown et al.* (Hrsg.) International Handbook on Whistleblowing Research, 2014, S. 232 ff.
27 *Ethics & Compliance Initiative* (Hrsg.), *Global Business Ethics Survey. Measuring Risk and Promoting Workplace Integrity*, 2016, S. 19; siehe dagegen aber *Bussmann/Niemeczek/Vockrodt*, MschrKrim 99/5 (2016), S. 32 f.
28 So etwa in den Jahren 2013 bis 2017 zwischen 13 % und 44 % bei *Ethics & Compliance Initiative* (Hrsg.), The State of Ethics & Compliance in the Workplace – Global Business Ethics Survey, 2018, S. 9; zwischen 1,9 % und 2,9 % bei *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 15 ff.; bis zu 80 % bei *Public Concern at Work* (Hrsg.), Whistleblowing: Time for Change, 2016, S. 7; *dies.*, Whistleblowing: the Inside Story, 2013, S. 16 ff.
29 *Public Concern at Work* (Hrsg.), Whistleblowing: the inside story, 2013, S. 3-4, 16-22; *Ethics Resource Center* (Hrsg.), Retaliation: When Whistleblowers Become Victims. A Supplemental Report of the 2011 National Business Ethics Survey, 2012, S. 7.
30 *Park/Bjørkelo/Blenkinsopp*, Journal of Business Ethics 23/4 (2018); *Rothschild*, Current Sociology 56/6 (2008), S. 890.
31 Z.B. hatten Klagen nach US- bzw. UK-Schutzgesetzen bisher eine überschaubare Erfolgsrate, siehe etwa *Herold*, Whistleblower 2016, S. 117 ff. m.w.N., Einschätzung eines interviewten Whistleblowers auf S. 284; *Public Concern at Work* (Hrsg.), Whistleblowing: Time for Change, 2016, S. 6; *Heumann* et al., Public Integrity 16/1 (2013/2014), S. 30 ff.; *Modesitt,* University of Kansas Law Review 62/1 (2013), S. 165 ff.
32 Siehe etwa *Kuehn*, Journalism 19/3 (2018), S. 402 ff.; *Di Salvo/Negro*, Journalism 17/7 (2016), S. 805 ff.; *Di Salvo,* Celebrity Studies 7/2 (2015), S. 289 ff.
33 Zum Folgenden *Vögele/Baudermann*, Medien & Kommunikationswissenschaft 64/4 (2016), S. 518-541.
34 Eine vom Whistleblower losgelöste Konzentration auf den offengelegten Missstand fand sich in 26 % der Artikel. Die Rolle des Whistleblowers rückte hier in den Hintergrund, blieb neutral und wurde nicht bewertet.

Diese schillernde mediale Präsenz lässt sich als Ausdruck einer verbreiteten Haltung begreifen, für die Whistleblowing ein ambivalentes und janusköpfiges Verhalten ist, dessen Einordnung perspektiven- und interessenabhängig von der Helden- bis zur Schurkengeschichte reicht. Dabei wird speziell für Deutschland häufig eine moralisierende bis skeptische Haltung unterstellt, die sich aus historischen Denunziationserfahrungen speisen soll.[35] Eine empirische Bestätigung dieser Annahmen steht bislang aber noch aus.[36]

V. Was bringen Whistleblowing-Systeme?

1. Problemlage

Seit einigen Jahren geht man vielerorts dazu über, sich nicht einfach nur auf die (zufällige) Eigeninitiative von Whistleblowern zu verlassen und deren Informationen entgegenzunehmen, sondern ihnen spezielle, auf sie zugeschnittene Meldemöglichkeiten bereitzustellen. Angeboten werden in der Regel verschiedene Möglichkeiten der Kontaktaufnahme, typischerweise eine Telefon-Hotline, ein verschlüsseltes Internet-System, konventionelle Post- und E-Mail-Adressen oder direkt/anonym ansprechbare Ombudspersonen.[37] Dies zielt in sämtlichen Spielarten darauf ab, Insidern ihre Hemmungen und Ängste zu nehmen oder zumindest soweit abzubauen, dass sie sich für eine Meldung entscheiden. Gerade dort, wo man sich mit seinem Wissen auch anonym melden kann, soll ein risikoloser Weg der Informationsweitergabe offeriert werden – um auf diese Weise einen Zuwachs an Hinweisen und Missstandsenthüllungen zu stimulieren.[38] Daher werden derartige Hinweisgebersysteme von Teilen der Presse,[39] manchen Polizeieinheiten,[40] nicht wenigen anderen Kontrollbehörden[41] und zahllosen (vor allem größeren) Unternehmen eingeführt[42]. Dabei sollen die organisationseigenen Einrichtungen als „Frühwarnsystem“[43] der „Firmenhygiene“ dienen (und externes Whistleblowing letztlich unnötig machen)[44], während es bei den externen Systemen eher um Außenkontrolle und die Erlangung institutionell schwer zugänglicher Missstandsinformationen geht[45]. In beiden Varianten stellt sich – gerade auch, weil diese im Zuge der WB-RL zunehmend obligatorisch werden – die Frage, ob dies tatsächlich auch gut funktioniert.

2. Organisationseigene Whistleblowing-Systeme

Organisationseigene Whistleblowing-Systeme sind im zentraleuropäischen Raum relativ weit verbreitet. Den neuesten Erhebungen nach verfügen etwa 59 % – 66 % über eine eigene Meldestelle, wobei die Verbreitung allerdings stark abhängig von der Unternehmensgröße ist.[46] Um die (trotz dieser Verbreitung) nicht selbstverständliche Effektivität zu beurteilen, lassen sich insbesondere die Benchmark-Reports großer kommerzieller Anbieter von Hinweisgebersystemen heranziehen.[47] In der Datenbank, die weltweit die meisten Hinweise aus internen Whistleblowing-Systemen enthält, gingen im Jahr 2018 bei 2.738 Unternehmen und Organisationen jeweils mehr als 10 Meldungen ein (die relativen Werte betragen im Mittel maximal 1,4 Meldungen pro 100 Angestellte).[48] Eine andere Studie ermittelte bei 1.392 Unternehmen aus Deutschland, Frankreich, Großbritannien und der Schweiz eine durchschnittliche Meldeanzahl von 52 (65 bei Groß- und 16 bei Klein- und mittelgroßen Unternehmen).[49] Auf der Ebene von Einzelunternehmen berichtet bspw. Siemens etwa für 2018 von 647 Meldungen, die „weitere Sachverhaltsermittlungen oder Untersuchungen erforderten“.[50]

Der sich hierin abzeichnende Ertrag soll, so lauten jedenfalls verbreitete Erwartungen, durch bestimmte Ausgestaltungen der Hinweisgebersysteme beeinflusst werden können. Das betrifft einmal die Einführung von Schutzvorkehrungen und -garantien, die die Whistleblower vor Vergeltungsmaßnahmen bewahren. Die empirische Erkenntnislage ist aber auch an dieser Stelle uneindeutig, nicht zuletzt wegen der methodischen Schwächen der wenigen einschlägigen Studien.[51] Unter diesem Vorbehalt soll das Hinweisaufkommen aber durch diverse Elemente gesteigert werden können: namentlich durch eine anwenderfreundliche Ausgestaltung (etwa durch Hotlines als Mitteilungskanal[52] sowie klare und als fair empfundene Richtlinien[53]), aber wohl auch durch rechtliche Schutzregelungen[54] und eine Unternehmenspraxis, in der die Meldemöglichkeiten und -verfahren klar in der Belegschaft kommuniziert und trainiert werden[55]. Ähnlich soll es sich (nach einer etwas widersprüchlicheren Forschungslage) bei speziellen Ansprechpartnern verhalten, etwa professionell eingerichteten „Audit Committees“ [56], Ombudspersonen und anderen Dienstleistern.[57] Anonymität oder Vertraulichkeit wirken nur nach einem Teil der Studien meldungsfördernd.[58] Dagegen spricht auch nicht notwendigerweise der relativ hohe Anteil anonymer, intern registrierter (Erst-)Meldungen (zwischen 48 % und 65 %[59]), da hieraus nicht hervorgeht, dass die Anonymität das entscheidende Meldekriterium war. Ohnehin wird die Wirksamkeit von Anonymität von vornherein dadurch limitiert, dass die Hinweisgeberidentität nicht selten aus der gelieferten Information erschlossen oder über interne Netzwerke preisgegeben werden kann.[60] Zudem scheint die Validität offener Meldungen höher[61] und es besteht (daher) die Gefahr, dass anonymen Meldungen weniger Glaubhaftigkeit attestiert wird[62].

Ungeachtet solcher Ausgestaltungsfragen ist festzuhalten, dass interne Meldesysteme durchaus genutzt werden. Allerdings besteht Anlass, dies aus mehreren Gründen zu relativieren. Erstens ist zu berücksichtigen, dass es innerhalb der Unternehmen neben den Hinweisgebersystemen auch konventionelle Meldewege sowie etliche andere Aufdeckungsmechanismen gibt. Die meisten Missstände werden daher auch intern durch Kontrollen und systematische Überprüfungsverfahren entdeckt, z.B. durch offene Hinweise oder die interne Revision und sogar öfter auch zufällig.[63] Befragungen der deutschen Beratungsbranche zufolge habe die Entdeckung unternehmensintern bearbeiteter Compliance-Verstöße zu 5 % bis 8 % auf Meldungen in den Hinweisgebersystemen beruht.[64] Weitere Studien ermitteln hierfür Werte von 14 % bis 22 %, wobei ca. ein Fünftel der Unternehmen angeben, schon einmal Hinweise erhalten zu haben, die für die Entdeckung/Aufklärung entscheidend waren.[65] Demnach liegt es nahe, bei der Nutzung der Hinweisgebereinrichtung eher von einer Umlenkung oder Verlagerung von Meldungen auszugehen und nicht primär von einer Neuaktivierung der Insider.

Zweitens scheint es bei den eingehenden Hinweisen nicht besonders häufig um echte Delikte des Managements oder Unternehmens zu gehen. Zwar ist an 36 % bis sogar 81 % der internen Eingaben dergestalt etwas „dran“, dass sie eine interne Überprüfung der jeweiligen Informationen rechtfertigen[66] und der Anteil echten Missbrauchs liegt regelmäßig im (niedrigen) einstelligen Prozentbereich (für Deutschland bisweilen auch über 10 %)[67]. Aber andererseits machen Sachverhalte, die bspw. auf Korruption, Untreue, Buchhaltungs- und Bilanzdelikte hindeuten – und das sind die Delikte, zu deren Aufdeckung solche Systeme in erster Linie eingeführt werden – nach den meisten dazu durchgeführten Auswertungen offenbar nur ca. ein Fünftel der Meldungen aus, nicht selten auch weniger. In der Regel geht es stattdessen um Konflikte zwischen den Mitarbeitern – also Personalangelegenheiten aller Art, z.B. um Belästigungs- oder Mobbingvorwürfe, um Diskriminierung oder Diebstahl.[68]

35 So etwa *Schmolke*, ZGR 48/5 (2019), S. 884 f.; *Schemmel/Ruhmannseder/Witzigmann*, Hinweisgebersysteme, 2012, Kap. 1, Rn. 64 ff., 80 ff. m.w.N.; *Hefendehl,* in: *Böse/Sternberg-Lieben* (Hrsg.), Grundlagen des Straf- und Strafverfahrensrechts. Festschrift für Knut Amelung, 2009, S. 617 ff.; *Tinnefeld/Rauhofer,* DuD 32/11 (2008), S. 717 ff.

36 Siehe aber das gegenteilige Ergebnis einer kleinen Umfrage, die *Hefendehl* unter Studierenden vorgenommen hat und der zufolge 72,4 % von 526 Teilnehmer/-innen den Whistleblower als „Retter“ sehen – im Gegensatz zu 27,6 %, die ihn als „Verräter“ qualifizieren (https://strafrecht-online.org/archiv/2018/7/16/whistleblowing/).

37 Siehe z.B. *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 34 ff.; *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 39; damit entsprechen diese Systeme insofern bereits den Vorgaben der WB-RL gem. Art. 9 Abs. 2 bzw. übertreffen sie sogar.

38 Dazu bspw. *Denk*, Das BKMS®-Hinweisgebersystem. Mediengespräch 2016, S. 6 ff.; *Hefendehl,* in: *Böse/Sternberg-Lieben* (Hrsg.), Grundlagen des Straf- und Strafverfahrensrechts. Festschrift für Knut Amelung, 2009, S. 617 ff.; siehe auch *BKA* (Hrsg.), Bundeslagebild Korruption, 2019, S. 22; *Baur/Holle*, AG 62/11 (2017), S. 379; *Möhlenbeck*, CB 9/2013, S. 382 ff.; *Schemmel/Ruhmannseder/Witzigmann*, Hinweisgebersysteme, 2012, Kap. 3, Rn. 16 ff. m.w.N.

39 Etwa: https://www.zeit.de/administratives/2019-01/technologiebranche-whistleblower-suche.

40 Etwa: https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=lka149ni&language=ger.

41 Etwa BT-Drs. 19/1342, Anlage 2.

42 Stellvertretend https://www.deutschebahn.com/de/konzern/compliance/hinweise_geben-1191634.

43 *Schemmel/Ruhmannseder/Witzigmann*, Hinweisgebersysteme, 2012, Kap. 3, Rn. 16 f. m.w.N.

44 *Koch*, ZIS 3/10 (2008), S. 502; *Berndt/Hoppler,* BB 60/48 (2005), S. 2627 ff.; vgl. auch *Möhlenbeck*, CB 9/2013, S. 385.

45 *BKA* (Hrsg.), Bundeslagebild Korruption, 2019, S. 22; *Denk*, Das BKMS®-Hinweisgebersystem. Mediengespräch 2016, S. 4 ff.

46 *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 7, 17; *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 35 ff., 63.

47 Diese Dienstleister stellen ihren Kundenunternehmen die Infrastruktur entsprechender Meldesysteme zur Verfügung und werten die dort eingehenden Meldungen für die Reports aus.

48 Daten des kommerziellen Anbieters *NAVEX Global* (Internetseite, Telefon-Hotline, E-Mail, App, Postweg, persönliche Anlaufstelle) bei *Penman/Hathorne*, 2019 Ethics & Compliance Hotline & Incident Management Benchmark Report, S. 4, 9. Umfasst sind insgesamt 1.032.953 Meldungen bei über 44 Millionen Angestellten. Vgl. auch 3,3/1.000 bei *Expolink* (Hrsg.), Whistleblowing Benchmarking Report 2019, S. 7.

49 *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 9, 56.

50 *Siemens* (Hrsg.), Nachhaltigkeitsinformation 2018, S. 37.

51 Was meist auf einem fehlenden Vergleichsgruppendesign beruht. Vgl. zudem auch oben bei Fn. 15.

52 *Johansson/Carey,* Journal of Business Ethics 139/2 (2016), S. 397 ff.

53 V.a. dazu, wer was wann wie melden darf. Vgl. *Mannion et al.*, Health Services and Delivery Research 30/2018, S. 25 m.w.N.; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 131 f.; *Lewis/Vandekerckhove*: Does Following A Whistleblowing Procedure Make A Difference?, in: *dies.* (Hrsg.), Developments in Whistleblowing Research, 2015, S. 93 ff.; *Seifert/Stammerjohan/Martin,* Behavioral Research in Accounting 26/1 (2014), S. 163 ff.; *Barnett/Cochran/Taylor,* Journal of Business Ethics 12/2 (1993), S. 132 ff.

54 Positiv z.B. *Mechtenberg/Muehlheusser/Roider*, Whistleblower Protection: Theory and Experimental Evidence 2018, S 32; gemischt *Lee/Pittroff/Turner*, Journal of Business Ethics 2018, DOI: 10.1007/s10551-018-4023-y: bei deutschen Buchhaltern wirkungslos im Unterschied zu amerikanischen; *Brennan/Kelly*, The British Accounting Review 39/1 (2007), S. 76 f.

55 *Stöber/Kotzian/Weißenberger*, Business Research 12/2 (2019), S. 400 ff.; *Graaf*, International Public Management Journal 22/2 (2019), S. 221 ff.

56 *Lee/Fargher*, Auditing: A Journal of Practice & Theory 37/1 (2018), S. 184; *Graaf*, International Public Management Journal 22/2 (2019), S. 221 ff.

57 *Gao/Greenberg/Wong-On-Wing*, Journal of Business Ethics 126/1 (2015), S. 91 ff., 96; *Waldron,* The Effectiveness of Hotlines in Detecting and Deterring Malpractice in Organisations, 2012, S. 20 ff., 41 ff.

58 Übersichten m.w.N. bei *Lee/Xiao*, Journal of Accounting Literature 41 (2018), S. 40; *Gao/Brink*, Journal of Accounting Literature 38 (2017), S. 5 ff.; ferner *Bussmann/Niemeczek/Vockrodt*, MschrKrim 99/5 (2016), S. 32 f.; *Johansson/Carey,* Journal of Business Ethics 139/2 (2016), S. 397 ff.; *Taylor/Curtis*, Behavioral Research in Accounting 25/2 (2013), S. 21 f., 29; *Waldron*, The Effectiveness of Hotlines in Detecting and Deterring Malpractice in Organisations, 2012, S. 44; vgl. auch *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 21; *Ethics Resource Center* (Hrsg.), Inside the Mind of a Whistleblower, 2012, S. 5; kein Effekt außerdem z.B. bei *Schön*, Situative Einflussfaktoren auf das Meldeverhalten bei Korruption, 2016, S. 486; *Kaplan et al.*, Advances in Accounting 28/1 (2012), S. 88 ff.

59 *Penman/Hathorne*, 2019 Ethics & Compliance Hotline & Incident Management Benchmark Report, S. 21; *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 59; *The Network*, Corporate Governance and Compliance Hotline Benchmarking Report, 2015, S. 22 f.

60 Beispiele bei *Herold*, Whistleblower, 2016, S. 190 f., 288 f.; vgl. auch *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 59: bei 38 % der anonymen Erstmeldungen wird „im Verlauf des Bearbeitungsprozesses die Identität bekannt“.

61 Die mittlere Begründetheitsrate („Substantiation Rate“) betrug 2017/18 bei *Penman/Hathorne*, 2019 Ethics & Compliance Hotline & Incident Management Benchmark Report, S. 26 f. z.B. knapp 40 % bei anonymen und 50 % bei offenen Meldungen; vgl. auch *Waldron,* The Effectiveness of Hotlines in Detecting and Deterring Malpractice in Organisations, 2012, S. 37; siehe dagegen aber *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 16.

62 *Guthrie/Norman/Rose*, Behavioral Research in Accounting 24/2 (2012), S. 97 ff.; *Hunton/Rose*, Journal of Management Studies 48/1 (2011), S. 89 ff.; siehe auch die Ansichten bei *Sauer/Blum*, Personal 9/2011, S. 40; *Fritz,* Personalwirtschaft 12/2009, S. 29 f.

63 Siehe z.B. *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 27.

64 *PwC* (Hrsg.), Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016, S. 43.

65 *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 27, 39; *dies.*, Tatort Deutschland: Wirtschaftskriminalität in Deutschland 2016, S. 34.

66 *WhistleB, Whistleblowing Centre* (Hrsg.), WhistleB Annual Customer Study on Organisational Whistleblowing, 2019; *Penman/Hathorne*, 2019 Ethics & Compliance Hotline & Incident Management Benchmark Report, S. 24; *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 58; *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 4 f., 7, 10, 14, 22 f.; *PwC* (Hrsg.), Compliance und Unternehmenskultur, 2010, S. 34 f.

67 *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 58; *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 38; *PwC* (Hrsg.), Wirtschaftskriminalität 2018, S. 4, 45; *dies.* (Hrsg.), Compliance und Unternehmenskultur, 2010, S. 34 f.

68 *Penman/Hathorne*, 2019 Ethics & Compliance Hotline & Incident Management Benchmark Report, S. 4, 14 ff.; *Expolink* (Hrsg.), Whistleblowing

Drittens liegen keine tragfähigen Studien zu der Frage vor, was mit den eingegangenen Hinweisen in den Unternehmen geschieht. Dass die mitgeteilten Missstände tatsächlich ausermittelt und aufgearbeitet werden und dass man sodann Vorkehrungen zu ihrer künftigen Vermeidung trifft, ist nur bedingt empirisch nachvollziehbar. Dies beruht nicht zuletzt darauf, dass sich die Unternehmen sehr bedeckt halten und nur sehr vage Angaben zu ihrem Umgang mit Missstandshinweisen machen. Sie veröffentlichen nur selten die Konsequenzen, die sie aus den gemeldeten Missständen ziehen.[69] Der „Integrierter Bericht 2018" der Deutschen Bahn spricht z.B. lediglich davon, dass „Korruptionsfälle im zweistelligen Bereich zentral über das Hinweismanagement eingegangen und geprüft" und erforderliche „Abhilfemaßnahmen […] eingeleitet" wurden.[70] Nach einer der wenigen einschlägigen Unternehmensbefragungen haben intern untersuchte Problemlagen – die indes nur in 14 % durch Hinweisgebersysteme/Ombudsleute bekannt geworden waren – aber immerhin zu 74 % bis 78 % zu „Veränderung der Präventionsmaßnahmen", in 60 % bis 66 % zu „organisatorischen Maßnahmen/Strukturveränderungen", in 42 % bis 49 % zu „personellen Veränderungen bei den Verantwortlichen/Zuständigkeiten" und in 26 % zur Meldung an die Aufsicht geführt.[71] Nicht selten besteht die interne Hinweisbearbeitung jedoch eher nur aus personellen Maßnahmen gegen die Verantwortlichen (Kündigungen oder sonstige Disziplinarmaßnahmen).[72] Dies korrespondiert mit der generellen Tendenz von Organisationen, Compliance-Verstöße vorwiegend als personelle und weniger als strukturelle Probleme zu kommunizieren.[73]

Nach manchen Studien scheinen interne Anlaufstellen die ihnen zugehenden Meldungen weniger ernsthaft als externe Empfänger in Ermittlungen einmünden zu lassen.[74] Ähnliche Hinweise ergeben sich auch aus Befragungen, die mit Whistleblowern zum Umgang mit ihren Meldungen durchgeführt wurden. Bei der UK-Whistleblower-Hilfs- und Beratungsorganisation *Public Concern at Work* (PCaW, seit 10/2018 umbenannt in „Protect") schilderten die Befragten, dass die Standard-Reaktion ihrer Organisationen darin bestand, nichts in Bezug auf die Meldung zu unternehmen. Nur etwa jeder Dritte berichtete bis 2015 davon, dass der gemeldete Missstand zugegeben und/oder beseitigt wurde, wobei die Quote interner Untersuchungen mit mehrfachen internen Versuchen stieg.[75] In Norwegen berichteten indes studienübergreifend ca. 36 % bis 71 % der meist internen Whistleblower von einer vollständigen oder teilweisen Missstandsbehebung.[76] Es ist daher alles andere als unwahrscheinlich, dass manche Meldung unter den Tisch fällt oder in einer Weise behandelt wird, die man sich von Rechts wegen anders vorstellen könnte. In Zukunft werden Organisationen allerdings dazu verpflichtet sein, Whistleblowern nicht nur eine Eingangsbestätigung ihrer Meldung zukommen zu lassen, sondern gem. Art. 9 Abs. 1 b), f) WB-RL spätestens nach drei Monaten auch zu kommunizieren, was daraus geworden ist. Ob dann in bestimmten, betriebswirtschaftlich opportunen Fällen lediglich „Formrückmeldungen" versandt werden, muss sich zeigen.

3. Externe Whistleblowing-Systeme der Behörden

Die Funktionalität externer Hinweisgebereinrichtungen zu beurteilen, erweist sich als noch schwieriger. So ist es kaum möglich, einen Überblick über die Vielzahl und erhebliche Vielfalt solcher Systeme zu erlangen. Speziell die externen Whistleblowing-Systeme im deutschen Sprachraum scheinen allerdings in der Praxis ohnehin oft ein Schattendasein zu führen und kaum in Anspruch genommen zu werden. Bei etlichen Einrichtungen deutscher Bundesbehörden gehen so wenige Meldungen ein, dass gar keine gesonderte Auswertung erfolgt (etwa bei der Generalzolldirektion).[77] Das Bundeskartellamt erhält seit 2012 durchschnittlich etwa 300 Hinweise pro Jahr, bei der BaFin stiegen die Eingaben von 123 (2016) über 629 (2017) auf 665 (2018).[78] Die meisten Meldungen registrieren die Fehlverhaltensbekämpfungsstellen der gesetzlichen Krankenkassen (deutschlandweit im Zeitraum 2016/2017 insgesamt 33.041 wovon sie 3.371 an die Staatsanwaltschaften weiterleiteten).[79] In der Gesamtschau bleibt aber erneut vieles unklar, auch was die tatsächliche Informationsnutzung betrifft. Bei der Bewertung dieser Zahlen ist zudem zu berücksichtigen, dass es sich hierbei jeweils nur um Meldesysteme für bestimmte, teilweise eng begrenzte Sektoren handelt (etwa

Benchmarking Report 2019, S. 10 f.; *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 12; *Lewis/Kender*, A Survey of Whistleblowing/Confidential Reporting Procedures in the UK top 250 FTSE Firms, 2010, S. 20; vgl. auch *WhistleB Whistleblowing Centre* (Hrsg.), WhistleB Annual Customer Study on Organisational Whistleblowing, 2019. Siehe zudem *Statista* (Hrsg.), Illegale Praktiken am Arbeitsplatz 2017.

69 Bei *Hauser/Hergovits/Blumer*, Whistleblowing Report 2019, S. 53, gaben allein 8,7 % (Frankreich), 11,5 % (BRD), 12,2 % (Schweiz) und 16,3 % (UK) eine solche Praxis an.

70 *Deutsche Bahn* (Hrsg.), Integrierter Bericht 2018, S. 255.

71 *KPMG* (Hrsg.), Licht ins Dunkel bringen, 2018, S. 30, 39 f.; *dies.* (Hrsg.), Tatort Deutschland: Wirtschaftskriminalität in Deutschland, 2016, S. 37; siehe ergänzend *Smith/Brown*, in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 116, wo nur zu 20 % organisationelle Maßnahmen ergriffen wurden.

72 *The Network* (Hrsg.), 2015 Corporate Governance and Compliance Hotline Benchmarking Report, S. 4, 24 f. Für ähnliche Angaben siehe *Siemens* (Hrsg.), Nachhaltigkeitsinformation 2018, S. 37 f.; konkrete Beispiele bei *BASF* (Hrsg.), BASF-Bericht 2017, S. 136. Vgl. auch *PwC* (Hrsg.), Wirtschaftskriminalität 2018, S. 68.

73 Fn. 19.

74 So die Hinweise in der Auswertung britischer PCaW-Daten bei *Vandekerckhove/Phillips*, Journal of Business Ethics 159/1 (2019), S. 214.

75 *Vandekerckhove/Phillips*, Journal of Business Ethics 159/1 (2019), S. 213 ff.; aber 80 % schilderten einen für sie negativen Ausgang, *Public Concern at Work* (Hrsg.), Whistleblowing: Time for Change, 2016, S. 7, 11; *dies.* (Hrsg.), Whistleblowing: the inside story, 2013, S. 30; siehe auch die niedrigen Zufriedenheitsraten bei *Smith/Brown*, in: *Brown* (Hrsg.), Whistleblowing in the Australian public sector, 2008, S. 112 ff.

76 Bei lediglich 7 %–25 % Repressionsquote, siehe *Trygstad/Ødegård/Svarstad*, in: *Lewis/Vandekerckhove* (Hrsg.) Selected papers from the International Whistleblowing Research Network conference, 2017, S. 28 ff.; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 120 ff., 131 ff.

77 BT Drs. 19/14980, S. 22 ff.

78 BT Drs. 19/14980, S. 13, 17, Erkenntnisse zur Weiterverarbeitung liegen nicht vor.

79 BT Drs. 19/14980, S. 8 ff. Informationen über den weiteren Verfahrensverlauf liegen auch hier nicht vor.

das Gesundheitssystem oder Finanzwesen). Aufschlussreicher wären Daten zu sektorenübergreifenden Meldestellen, also in erster Linie der Polizei.

Diese verfügt schon insofern über ein faktisches Meldesystem, weil grundsätzlich jeder Organisationsinsider eine konventionelle Strafanzeige stellen kann (auch telefonisch, per E-Mail oder online).[80] Allerdings ist dann zu beachten, dass die Ermittlungsbehörden die Identität des Anzeigeerstatters häufig nicht vertraulich behandeln (können). So mag es bspw. erforderlich sein, einen Verdächtigen mit der Aussage des Insiders zu konfrontieren, was in der Regel dessen Benennung erforderlich macht. Sollte es im Weiteren zu einer Gerichtsverhandlung kommen, wird der Insider vielfach als Zeuge herangezogen – sei es auf Antrag der Staatsanwaltschaft oder der Verteidigung. Er muss dann erscheinen und auch aussagen (es sei denn, es besteht ausnahmsweise ein Befreiungsgrund).[81] Deshalb darf die Polizei dem Insider auch keine vollständige Vertraulichkeit versprechen, weil sie eine solche Zusage verfahrensrechtlich oftmals gar nicht einhalten kann. Sie ist dann vielmehr gezwungen, den Hinweisgeber ziehen zu lassen, wenn dieser unter solchen Umständen lieber keine Anzeige erstatten will. Zwar ist es auch ohne Weiteres möglich, eine Anzeige anonym zu übermitteln, etwa per Brief ohne Absender. Bei einem solchen Vorgehen ist aber damit zu rechnen, dass der Meldung wenig Glauben geschenkt wird.[82] Außerdem gehört es dann in der Regel zur polizeilichen Aufklärungspflicht, die Identität des Anzeigeerstatters trotzdem ermitteln zu müssen. Das ist häufig schon deshalb erforderlich, um die Tragfähigkeit der Mitteilung einschätzen zu können. Ferner ergeben sich oftmals inhaltliche Fragen, die die Polizei dann nicht per Rücksprache klären kann. Die Position des Insiders bleibt zudem, wenn er die Polizei kontaktiert, nach (noch) geltender Rechtslage durchgehend riskant, auch im Hinblick auf eine eigene Strafbarkeit, die sich z.B. aus der Beschaffung der Informationen[83] oder ihrer Weitergabe ergeben kann[84]. Eine Strafanzeige bildet für ihn daher alles in allem (wenn er nicht von vornherein offen auftreten will[85]) also keine attraktive Option. In der Konsequenz bleibt die Anzeigehäufigkeit bei Korruption und vielen anderen „opferlosen Heimlichkeitsdelikten" de facto notorisch gering.[86]

Daher sind zahlreiche Strafverfolgungs- und Kontrollbehörden dazu übergegangen, spezielle digitale Hinweisgebersysteme zu schalten (oft über die schon erwähnten, kommerziellen Drittanbieter).[87] Diese ermöglichen teilweise nicht nur einen aufwandsarmen Online-Kontakt, sondern auch eine technisch absolut gewährleistete Melder-Anonymität bei gleichzeitiger Dialogmöglichkeit (für Rückfragen, Dateienübermittlung, Fortgangsinformationen usw.).[88] Seitens einzelner Polizeibehörden liegen hierfür auch gewisse „Ertrags-Daten" vor. Beim Landeskriminalamt Niedersachsen, das ein solches System bereits seit Beginn der 2000er Jahre einsetzt, liegt das jährliche Meldungsaufkommen bei 200 bis 300. Darunter sind auch solche Anzeigen, die zu weiteren Abklärungen führen und/oder in strafrechtliche Ermittlungsverfahren münden. Die große Mehrheit wird allerdings ergebnislos eingestellt. Von den 2.729 im Zeitraum 01/2009 – 02/2019 eingegangenen Meldungen boten 32,39 % einen Anfangsverdacht, aber lediglich 1,14 % führten zu einer Verurteilung (bei 2,09 % noch offener Verfahren).[89] In Österreich, wo dasselbe System zur Wirtschaftsstrafverfolgung bundesweite Verwendung findet, verhält es sich ähnlich. Hier waren vom 01.04.2013 bis zum 31.03.2017 insgesamt 4.976 Meldungen eingegangen. Davon führten knapp 10,71 % zur Einleitung eines Ermittlungsverfahrens und nur 0,58 % zu einer Anklage. Hinzu kamen weitere ca. 2,5 % von Verfahren, die noch laufen bzw. in denen der Hinweis geeignet war, in ohnehin schon eröffneten Ermittlungsverfahren berücksichtigt zu werden. Insgesamt sind hier die Werte noch niedriger als in Niedersachsen.[90] Juristisch sind solche polizeilichen Hinweisgebersysteme ohnehin immer umstritten geblieben (Gründe u.a.: staatliche Motivierung zur Preisgabe geschützter Geheimnisse,[91] Erleichterung von Falschverdächtigungen).[92] Vom Gesetzgeber ist daher zu verlangen, bei der Umsetzung der WB-RL hier für eine Klärung zu sorgen (zumal die Handhabung völlig anonymer Meldungen durch Art. 6 Abs. 2 WB-RL der nationalen Gesetzgebung generell anheimgestellt wird).

80 Siehe das allgemeine Anzeigerecht in § 158 StPO, das in der Literatur bisweilen sogar als Whistleblowing-Rechtfertigungsnorm (über)interpretiert wird (dazu *Engländer/Zimmermann*, NZWiSt 9/2012, S. 330).

81 Siehe §§ 48 Abs. 1 S. 1, 70 StPO; vgl. auch § 161a Abs. 1 S. 1 StPO und das Akteneinsichtsrecht gem. § 147 StPO.

82 Vgl. Fn. 61, 62; siehe auch den Hinweis eines Staatsanwalts an das LKA Nds. bei *Backes/Lindemann*, Staatlich organisierte Anonymität als Ermittlungsmethode bei Korruptions- und Wirtschaftsdelikten, 2006, S. 48 Fn. 60.

83 Etwa nach §§ 202a/b/c StGB.

84 Etwa nach §§ 202, 353b StGB. Dazu bspw. *Schreiber,* NZWiSt 8/9 (2019), S. 332 ff.

85 Was aber gleichwohl die meisten (internen) Whistleblower zunächst tun, siehe *Vandekerckhove/Phillips*, Journal of Business Ethics 159/1 (2019), S. 209 ff.; *Skivenes/Trygstad,* Economic and Industrial Democracy 38/1 (2017), S. 121; *Public Concern at Work* (Hrsg.), Whistleblowing: Time for Change, 2016, S. 6.

86 *Schemmel/Ruhmannseder/Witzigmann*, Hinweisgebersysteme, 2012, Kap. 3, Rn. 28; *Koch,* ZIS 3/10 (2008), S. 501 f., siehe auch *Kölbel/Herold,* NK 16/4 (2015), S. 376.

87 Etwa die BaFin unter https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2BaF6&language=ger oder die Fehlverhaltensbekämpfungsstellen einiger gesetzlicher Krankenkassen, z.B. der KKH unter https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=118kkh&language=ger.

88 Für eine Beschreibung der Funktionsweise siehe etwa *Denk,* Das BKMS®-Hinweisgebersystem. Mediengespräch 2016, S. 5 f.

89 *LKA Niedersachen,* Abteilung 3, Dezernat 37 – Zentralstelle Korruption / Interne Ermittlungen, Auswertung BKMS-System vom 07.03.2019; eine Zusammenfassung älterer Daten bei *Herold,* in: Boers/Schaerff (Hrsg.), Kriminologische Welt in Bewegung, 2018, S. 236 f.

90 Siehe https://www.parlament.gv.at/PAKT/VHG/XXV/AB/AB_12165/imfname_638955.pdf; siehe auch *Denk,* Das BKMS®-Hinweisgebersystem. Mediengespräch 2016, S. 5 f.

91 Fn. 84.

92 Aus der kritischen Literatur z.B. *Auer*, CB 1/2013, S. 2; *Hefendehl,* in: *Böse/Sternberg-Lieben* (Hrsg.), Grundlagen des Straf- und Strafverfahrensrechts. Festschrift für Knut Amelung, 2009, S. 630; *Mahnhold*, NZA 25/13 (2008), S. 739 f.; *Backes/Lindemann*, Staatlich organisierte Anonymität als Ermittlungsmethode bei Korruptions- und Wirtschaftsdelikten, 2006, S. 102 ff.

VI. Ausblick

Aus diesen empirischen Funktionalitäts-Erkenntnissen folgt noch eine andere Problematik von eher kriminalpolitischer Art. Man kann sich nämlich fragen, ob es klug ist, wenn von gesetzgeberischer Seite neben den eigenen staatlichen Hinweisgebersystemen auch noch die der Unternehmen stark gemacht werden. Denn genau das geschieht ja, indem man die Unternehmen zu deren Einrichtung verpflichtet und damit gewissermaßen die eigene Konkurrenz stärkt.[93] Je besser diese internen Meldeeinrichtungen funktionieren, desto eher werden eben diese Systeme von den Insidern genutzt, und gerade nicht die der Behörden. Vielfach wird dann aber auch nur eine unternehmensinterne Verarbeitung der mitgeteilten Informationen erfolgen. Und diese Verarbeitung ist am Interesse des Unternehmens orientiert – also an einem Interesse, das sich nicht notwendig mit den Belangen des Gemeinwohls decken muss.[94] Dass die EU dieses Nebeneinander von internen und externen Whistleblowing-Einrichtungen dennoch nachdrücklich forciert (Art. 7 Abs. 2 WB-RL, Art. 8-12), beruht auf dem Vertrauen, das sie – im Unterschied zur kritischen Literatur – in die Selbstregulierung der Unternehmen hat.[95] Insofern muss man es schon als Fortschritt begreifen, dass die WB-RL keinen Vorrang von Meldungen über interne Systeme vorsieht, sondern Hinweisgebern die Wahl zwischen den organisationseigenen und externen, behördlichen Meldekanälen lässt (Art. 10).[96]

93 Bei der Umfrage von *Ternes*, Der Konzern 17/3 (2019), S. 117 fehlt z.B. bei 62,5 % nicht börsennotierter Unternehmen nämlich ein Hinweisgebersystem noch.
94 Näher zu dieser Problematik *Kölbel/Herold*, MschrKrim 93/6 (2010), S. 431 ff. m.w.N.
95 Erwägungsgrund 33, in: Amtsblatt L 305 der EU 62 (26.11.2019), S. 23. Eingehend zu den verschiedenen Sichtweisen auf Unternehmen, deren Delinquenz und Selbstregulierungsfähigkeit etwa *Kölbel*, MschrKrim 100/6 (2017), S. 430 ff.
96 Kritisch dazu etwa *Schmolke*, ZGR 48/5 (2019), S. 906 ff., 922; *Hiéramente/Ullrich*, jurisPR-StrafR 25/2019 Anm. 1. Als letzte Möglichkeit bleibt die Offenlegung gem. Art. 15.

Vortrag zur Veranstaltung
Prof. Dr. Martin Franzen, LMU München

Arbeits- und datenschutzrechtliche Fragen des „Whistleblowing“

I. Einleitung

1. Begriff des „Whistleblowing“

Mein Thema lautet: „Arbeits- und datenschutzrechtliche Fragen des Whistleblowing“. Ganz allgemein versteht man unter „Whistleblowing“ im hier interessierenden unternehmensbezogenen Kontext kritische Äußerungen, Beschwerden oder Anzeigen von abhängig Beschäftigten über Missstände oder Fehlverhalten im Unternehmen.[1] Man kann weiter „internes“ und „externes“ Whistleblowing unterscheiden: Internes „Whistleblowing“ liegt vor, wenn der Arbeitnehmer vermeintliche oder bestehende Missstände gegenüber seinem Arbeitgeber bzw. den von diesem vorgesehenen Stellen darlegt. Beim sogenannten „externen“ Whistleblowing wendet sich der Mitarbeiter an außenstehende Dritte, etwa an die Staatsanwaltschaft oder andere zuständige Behörden, Gewerbeaufsicht, Datenschutzbehörde etc. je nach Zuständigkeit und Interesse.

2. Das Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) vom 21.7.2011 in der Rechtssache Heinisch/Deutschland

Es ging um die Kündigung einer Altenpflegerin – Frau Heinisch – in einem von *Vivantes* betriebenen deutschen Altenpflegeheim – *Vivantes* ist ein Unternehmen, das im Eigentum des Landes Berlin steht. Im Jahr 2002 stellte der Medizinische Dienst der Krankenkasse schwerwiegende Missstände in der täglichen Pflege in dem Altenheim fest, in dem Frau Heinisch beschäftigt war. Für diese Probleme wurde die in dem Pflegeheim bestehende Personalknappheit verantwortlich gemacht. In der Zeit zwischen Januar 2003 und Oktober 2004 unterrichteten sowohl Frau Heinisch als auch ihre Kollegen mehrmals die Leitung des Pflegeheims über die Überbelastung des Pflegepersonals sowie über die Defizite in der Pflege und der Dokumentierung der Pflegeleistungen. In einer Mitteilung an ihren Arbeitgeber erwähnte Frau Heinisch überdies, dass sie nicht länger in der Lage sei, die Verantwortung für die Missstände in der Altenpflege zu übernehmen. Seit Mai 2003 war sie wiederholt arbeitsunfähig krank. Eine weitere Visite des Pflegeheims durch den Medizinischen Dienst der Krankenkasse ließ im November 2003 erneut gravierende Missstände in der Pflege zu Tage treten, die auch auf die Personalknappheit beim Arbeitgeber zurückzuführen waren. Nach mehreren weiteren Meldungen von Missständen in der Pflege an ihre Vorgesetzten (insbesondere im Oktober 2004) wurde Frau Heinisch erneut arbeitsunfähig krank und konsultierte einen Rechtsanwalt. Dieser wandte sich nach abermaligem Hinweis auf die Missstände und ergebnisloser Androhung einer Strafanzeige dann tatsächlich an die Staatsanwaltschaft. Anfang 2005 stellte die Staatsanwaltschaft Berlin das Ermittlungsverfahren gegen den Arbeitgeber nach § 170 Abs. 2 StPO ein. In der Folgezeit erfuhr *Vivantes* davon, dass die Strafanzeige auf die Beschwerdeführerin zurückging. Das Unternehmen kündigte daraufhin nach ordnungsgemäßer Anhörung des Betriebsrats das Arbeitsverhältnis wegen der gegen *Vivantes* erstatteten Strafanzeige.

Die Kündigungsschutzklage von Frau Heinisch war vor dem ArbG Berlin[2] erfolgreich, nicht aber vor dem LAG Berlin[3]. Das LAG sah in der Erstattung einer Strafanzeige gegen *Vivantes* durch die Beschwerdeführerin einen wichtigen Grund i. S. d. § 626 Abs. 1 BGB, der die Arbeitgeberin zur außerordentlichen Kündigung berechtigte. Die gegen die Nichtzulassung der Revision eingelegte Nichtzulassungsbeschwerde hat das *BAG* durch Beschluss vom 6. Juni 2007[4] zurückgewiesen. Die von der Beschwerdeführerin eingelegte Verfassungsbeschwerde wurde vom *BVerfG* nicht zur Entscheidung angenommen.[5] Die hier gegen gerichtete Beschwerde zum EGMR war erfolg-

1 Siehe *Schulz*, BB 2011, 629, 630 m.w.N.

2 ArbG Berlin 3.8.2005 – Az. 39 Ca 4775/05 (n. v.).
3 LAG Berlin 28.3.2006 - 7 Sa 1884/05, ArbuR 2007, 51 = LAGE Nr. 7b zu § 626 BGB 2002 (*Ulber*); vgl. auch die Anm. zu der LAG-Entscheidung von *Binkert*, ArbuR 2007, 197 ff. sowie von *Deiseroth*, ArbuR 2007, 198 ff.
4 BAG 6.6.2007 – 4 AZN 487/06 (n. v.).
5 BVerfG 6.12.2007 – 1 BvR 1905/07 (n. v.).

reich: Die 5. Kammer des EGMR hat in ihrer Entscheidung vom 21.7.2011 einstimmig festgestellt, dass eine Verletzung des Grundrechts von Frau Heinisch auf Meinungsfreiheit aus Art. 10 EMRK vorliegt.

3. Internes und externes Whistleblowing

Der geschilderte Sachverhalt illustriert aus meiner Sicht anschaulich die Zusammenhänge von internem und externem „Whistleblowing“: Nach allem, was wir aufgrund der mitgeteilten Tatbestände wissen, hat Frau Heinisch auf Missstände intern aufmerksam gemacht. Diese wurden aber aus welchen Gründen auch immer nicht abgestellt. Erst danach hat sie sich an die Staatsanwaltschaft gewandt – möglicherweise leichtfertig, weil Personalknappheit als solche nun keinen strafrechtlich relevanten Anfangsverdacht begründet.

Andererseits: Wenn Unternehmen den Mitarbeitern das Gefühl geben, ihre Anliegen und Beschwerden seien bei dem Unternehmen gut aufgehoben, wenn es also Mechanismen im Unternehmen für internes „Whistleblowing“ gibt, dann verringert sich die Gefahr für das Unternehmen, dass sich der Arbeitnehmer an externe Stellen wendet, also zum „externen Whistleblowing“ greift. Unternehmen haben also ein ureigenes Interesse daran, interne Verfahren zu etablieren, in denen sich Mitarbeiter offenbaren können. Dadurch können externe Stellen und Aufsichtsbehörden zunächst aus dem Unternehmen herausgehalten werden.

Es bestätigt sich der vom deutsch-amerikanischen Ökonomen *Hirschman* herausgearbeitete Zusammenhang zwischen „voice“, „loyalty“ und „exit“: Wer der Möglichkeit, Beschwerden anzubringen („voice“), keinen Raum gibt, riskiert die Folgebereitschaft der Mitarbeiter („loyalty“) und fördert gegebenenfalls die Abwanderung („exit“) oder in unserem Kontext „externes“ Whistleblowing. Dies ruft dann unter Umständen staatliche Behörden oder bei hinreichender Skandalisierungsfähigkeit die Öffentlichkeit auf den Plan.

4. Gang der Überlegungen

Zunächst möchte ich mich mit arbeitsvertragsrechtlichen Fragen des „Hinweisgebens“ auseinandersetzen (II). Im Anschluss daran werde ich datenschutzrechtlichen Fragen in Zusammenhang mit Hinweisgebersystemen nachgehen (III). Ich werde das auf der Basis des derzeit geltenden Rechts tun unter weitgehender Ausblendung der durch die Hinweisgeberrichtlinie möglicherweise angestoßenen Veränderungen.

II. Arbeitsvertragsrecht

Im Bereich des Arbeitsvertragsrechts stellen sich insbesondere zwei Grundfragen: In welchem Umfang ist der Arbeitnehmer verpflichtet, dem Arbeitgeber Rechtsverstöße und ähnliche Vorkommnisse anzuzeigen (internes „Whistleblowing“)? Und zweitens: Unter welchen Voraussetzungen darf der Arbeitnehmer sich an außenstehende Dritte – etwa Aufsichtsbehörden oder Staatsanwaltschaft wenden (externes „Whistleblowing“)?

1. Meldepflicht des Arbeitnehmers gegenüber dem Arbeitgeber

a) Ausprägung der allgemeinen Rücksichtnahmepflicht (§ 241 Abs. 2 BGB)

Eine allgemeine gesetzliche Verpflichtung des Arbeitnehmers, seinen Arbeitgeber bzw. Vorgesetzten über das Fehlverhalten anderer Arbeitnehmer zu informieren, existiert nicht. Insoweit einschlägige gesetzliche Regelungen finden sich lediglich im Arbeitsschutzrecht in § 16 Abs. 1 ArbSchG. Danach müssen die Beschäftigten dem Arbeitgeber oder zuständigen Vorgesetzten jede von ihnen festgestellte unmittelbare erhebliche Gefahr für die Sicherheit und Gesundheit sowie jeden an den Schutzsystemen festgestellten Defekt unverzüglich melden.

Eine entsprechende arbeitsvertragliche Pflicht kann somit lediglich als Ausprägung der allgemeinen vertragsrechtlichen Rücksichtnahmepflicht (§ 241 Abs. 2 BGB) als Nebenpflicht des Arbeitnehmers entwickelt werden. Die Rechtsprechung des BAG ist in diese Richtung bereits in lange zurückliegenden Entscheidungen gegangen und hat hierbei auf die Treuepflicht des Arbeitnehmers abgestellt. Das Fallmaterial aus der höchstrichterlichen Rechtsprechung zur Konkretisierung einer solchen Pflicht, Rechtsverstöße anderer Arbeitnehmer gegenüber dem Arbeitgeber oder seinen Vertretern zu melden, ist allerdings spärlich. Man kann die in Rechtsprechung und Literatur hierzu gewonnenen Erkenntnisse in drei Fallgruppen zusammenfassen:

Führungskräfte sind zu einer entsprechenden Meldung verpflichtet, wenn die Überwachung und Kontrolle anderer Arbeitnehmer zu ihren Aufgaben gehört.[6] Bei anderen Arbeitnehmern hat die Rechtsprechung eine derartige Meldepflicht bejaht, wenn das Vorkommnis einen Bezug zum Aufgabenkreis des Arbeitnehmers aufweist und Wiederholungsgefahr besteht.[7] Ohne Bezug zum Aufgabenkreis des Arbeitnehmers bejahen Teile der Literatur eine Meldepflicht, wenn dem Arbeitgeber durch den zu meldenden Pflichtverstoß des Dritten ein erheblicher Schaden droht.[8] Die Gegenauffassung lehnt jede Meldepflicht des Arbeitnehmers außerhalb von dessen Aufgabenbereich ab: Der Arbeitnehmer sei lediglich innerhalb seiner Leistungspflichten und damit innerhalb seines Aufgabenbereichs zur Schadensabwendung und daher auch Anzeige an den Arbeitgeber verpflichtet.[9] Die Grenze jeglicher Meldepflicht zieht der BGH dort, wo der Arbeitnehmer sich selbst einer eigenen Vertragsverletzung bezichtigen müsste;[10] die Meldepflicht kann also niemals zu einer Selbstanzeigepflicht führen.

6 Siehe BAG 12.5.1958 – 2 AZR 539/56 – AP Nr. 5 zu § 611 BGB Treuepflicht.
7 Siehe BAG 18.6.1970 – 1 AZR 520/69 – NJW 1970, 1861.
8 Siehe *Müller-Glöge*, in Münchener Kommentar zum BGB, 6. Aufl. 2012, § 611 BGB Rn. 1082.
9 *Boemke*, AR-Blattei SD 1228 Rn. 163 f.
10 BGH 23.2.1989 – IX ZR 236/86 – NJW-RR 1989, 614 Rn. 23 f.

b) Erweiterung der Meldepflicht durch Weisungsrecht (§ 106 GewO)?

Nach wohl allgemeiner Auffassung in der Literatur kann die skizzierte Meldepflicht durch Weisungsrecht konkretisiert werden, etwa dergestalt, dass den Arbeitnehmer Verfahrensvorgaben gemacht werden – also etwa wo, wann und wie zu melden ist. Dies schließt die Benutzung eines Hinweisgebersystems ein. Demgegenüber lehnt die Literatur eine materiellrechtliche Erweiterung der Meldepflicht aufgrund arbeitgeberseitiger Weisung überwiegend ab, weil aufgrund des Direktionsrechts des Arbeitgebers nicht neue Pflichten begründet werden könnten.[11] Außerdem würde eine aufgrund Direktionsrecht statuierte Verpflichtung des Arbeitnehmers, jegliches Fehlverhalten von Kollegen zu melden, den Arbeitnehmer unbillig belasten. Dem Arbeitnehmer ist es über die vorstehend skizzierten Grundsätze hinaus nicht zumutbar, Arbeitskollegen „anschwärzen“ zu müssen.

c) Erweiterung der Meldepflicht durch Allgemeine Geschäftsbedingungen (§§ 305 ff. BGB)

Eine Erweiterung der Meldepflicht über die vorstehend entwickelten Grundsätze hinaus durch AGB erscheint denkbar, muss sich allerdings der Inhaltskontrolle nach § 307 BGB stellen und darf daher nicht zu einer unangemessenen Benachteiligung des Arbeitnehmers führen. Man wird hierbei als maßgebliche Kriterien die Funktion des Arbeitnehmers und die Bedeutung des Regelverstoßes heranziehen können. Je höher der Arbeitnehmer in der Hierarchieebene des Unternehmens angesiedelt, desto eher ist ihm zuzumuten, alle Regelverstöße zu melden, unabhängig von Überwachungsaufgabe und Bezug des Regelverstoßes zu seinem Arbeitsbereich. Und weiter: Je gewichtiger der Regelverstoß, desto eher ist es auch allen Arbeitnehmern zuzumuten, diesen zu melden, unabhängig vom eingetretenen oder zu befürchtenden Schaden. So soll nach einer in der Literatur vertretenen Auffassung eine alle Arbeitnehmer betreffende Pflicht, Regelverstöße im Sinne des § 130 OWiG zu melden, durch AGB nach § 307 BGB wirksam statuiert werden können.[12] Darüber hinaus sollen auch Straftaten zu Lasten des Unternehmens selbst erfasst werden können.[13] Diese Überlegungen zeigen freilich, dass die arbeitsvertragliche Meldepflicht durch AGB nur maßvoll erweitert werden kann. Außerdem müsste dem Transparenzgebot im Sinne eines Bestimmtheitsgrundsatzes durch klare Benennung der jeweiligen Regelverstöße Genüge getan werden.

d) Exkurs: Auskunftspflicht

Von der Meldepflicht zu unterscheiden ist die Pflicht eines Arbeitnehmers, auf eine konkrete Anfrage des Arbeitgebers Auskunft zu geben. Mit dieser Fragestellung ist allerdings der Problemkreis des „Whistleblowing“ im engeren Sinne strengenommen verlassen und das sich daran gewissermaßen anschließende Gebiet der sogenannten internen Ermittlungen („internal investigations“) betreten. Deshalb möchte ich hierzu nur noch ganz kurz die Richtung der herrschenden Auffassung andeuten:

Die herrschende Auffassung differenziert folgendermaßen: Der Arbeitnehmer ist umfassend zur Auskunft verpflichtet, wenn sein eigener Arbeitsbereich betroffen ist. Dies folgert man aus § 666 BGB. Die Auskunftspflicht besteht auch, wenn sich der Arbeitnehmer selbst belasten muss.[14] Außerhalb des eigenen Aufgabenbereichs muss man die Grundsätze des Fragerechts des Arbeitgebers im Begründungsstadium des Arbeitsverhältnisses anwenden.[15] Der Arbeitnehmer muss also zutreffend Auskunft geben, wenn der Arbeitgeber für die Informationserhebung ein berechtigtes, billigenswertes Interesse hat und die zutreffende Beantwortung der entsprechenden Fragen dem Arbeitnehmer zumutbar ist. Dies wird man bejahen können, wenn die Fragen der Aufklärung arbeitsvertraglicher Pflichtverletzungen und gegebenenfalls Straftaten im Unternehmen dienen. Als Rechtsproblem stellt sich dann folgende Frage: Lässt der Umstand, dass ein Selbstbezichtigungsgebot nicht besteht, die Auskunftspflicht von vornherein entfallen,[16] oder nimmt man analog § 97 Abs. 1 S. 3 InsO bzw. § 630c BGB ein strafprozessuales Verwertungsverbot[17] an? In jedem Fall ist aber § 26 BDSG zu beachten.

e) Sanktionen

Als Verstoß gegen die Meldepflicht des Arbeitnehmers kommt eine verhaltensbedingte Kündigung wegen Verletzung der Meldepflicht in Betracht. Eine außerordentliche Kündigung setzt eine schwerwiegende und erhebliche Pflichtverletzung voraus. Hier wird man wieder die skizzierten drei Fallgruppen fruchtbar machen können: Führungskräfte unterliegen wegen der Überwachungspflicht der ihnen zugewiesenen Mitarbeiter einer gesteigerten Meldepflicht; hier kann eine außerordentliche Kündigung je nach Einzelfall in Betracht kommen. Bei den anderen Arbeitnehmergruppen dürfte der Verstoß gegen die Meldepflicht wohl regelmäßig nicht schwerwiegend genug sein. Es bleibt dann im Regelfall nur die ordentliche Kündigung, die in diesen Fällen stets auch eine Abmahnung voraussetzt.

Auf der subjektiven Seite muss der Arbeitnehmer schuldhaft gehandelt haben. Daran kann es fehlen oder der Schuldvorwurf wiegt nicht sehr stark, wenn dem Arbeitnehmer nicht bewusst war, dass er einer Meldepflicht unterliegt. Man wird hier bisweilen einen vermeidbaren oder sogar unvermeidbaren Verbotsirrtum zugunsten des Arbeitnehmers berücksichtigen müssen.

Insgesamt wird man sagen müssen, dass eine Kündigung als Sanktion für den Verstoß gegen die Meldepflicht wohl nur

11 Ebenso *Köstner*, Compliance-Richtlinien im Unternehmen, 2012, S. 170; *Schuster/Darsow*, NZA 2005, 273, 276; *Mengel/Hagemeister*, BB 2007, 1386, 1389.
12 *Mahnhold*, NZA 2008, 737, 739.
13 *Köstner*, Compliance-Richtlinien in Unternehmen, 2012, S. 172 f.
14 Ausdrücklich zu § 666 BGB: BGH 30.4.1964 – VII ZR 156/62 – BHGZ 41, 318 Rn. 24 (juris); BGH 30.11.1989 – III ZR 112/88 – NJW 1990, 510, 511.
15 Vgl. BAG 7.9.1995 – 8 AZR 828/93 – NZA 1996, 637.
16 So *Göpfert/Merten/Siegrist*, NJW 2008, 1703, 1705; a. A. BGH 30.4.1964 – VII ZR 156/62 – BGHZ 41, 318; BGH 30.11.1989 – III ZR 112/88 – NJW 1990, 511.
17 Dazu *Franzen*, in: Festschrift Köhler, 2014, S. 133, 140 ff.

in außergewöhnlichen und schweren Fällen mit Erfolg ausgesprochen werden kann. So ist das Fallmaterial aus der Rechtsprechung zu Kündigungen wegen Meldepflichtverletzungen sehr spärlich, was diesen Befund belegen dürfte.

Denkbar ist ferner eine Abmahnung; Schadensersatz nur, wenn das Verhalten des Arbeitnehmers zurechenbar einen Schaden verursacht hat, woran es regelmäßig fehlen wird.

2. Zulässigkeit von Hinweisen gegenüber außenstehenden Stellen (externes „Whistleblowing“)

Unter welchen Voraussetzungen darf sich der Arbeitnehmer an externe Stellen wenden, um auf Rechtsverstöße im Bereich des Arbeitgebers hinzuweisen?

a) Gesetzliche Regelung im Arbeitsschutzrecht: § 17 Abs. 2 ArbSchG

Eine gesetzliche Regelung dieses Problembereichs existiert ausschnittsweise wiederum im Arbeitsschutzrecht: Nach § 17 Abs. 2 ArbSchG können sich Beschäftigte an die zuständige Behörde wenden, wenn sie auf Grund konkreter Anhaltspunkte der Auffassung sind, dass die vom Arbeitgeber getroffenen Maßnahmen und bereitgestellten Mittel nicht ausreichen, um die Sicherheit und den Gesundheitsschutz bei der Arbeit zu gewährleisten, und der Arbeitgeber dem nicht abgeholfen hat. Der Gesetzgeber hat also im Arbeitsschutzrecht den Vorrang des innerbetrieblichen Abhilfeversuchs festgeschrieben.

b) Grundsätze der BAG-Rechtsprechung

Dies gilt ebenso nach der bisherigen Rechtsprechung des BAG außerhalb des engeren Bereichs des Arbeitsschutzrechts. Die vom BAG aufgestellten Grundsätze lassen sich wie folgt zusammenfassen: Der Arbeitnehmer muss, bevor er sich an eine außenstehende Stelle wendet, eine innerbetriebliche Abhilfe versuchen, soweit eine solche dem Arbeitnehmer zugemutet werden kann. Unzumutbar ist ein Versuch innerbetrieblicher Abhilfe dann, wenn sich der Arbeitnehmer selbst strafbar machen würde, falls er den Gesetzesverstoß nicht anzeigt.[18] Außerdem ist eine vorherige innerbetriebliche Klärung nicht mehr erforderlich, wenn innerbetriebliche Abhilfe nicht erwartet werden kann, weil der Arbeitnehmer den Arbeitgeber auf die Regelverstöße bereits hingewiesen hat, dieser sie aber nicht abgestellt hat. Der Vorrang innerbetrieblicher Abhilfe gilt ferner dann nicht, wenn die Vorfälle schwerwiegend sind und/oder sich der Verdacht gegen den Arbeitgeber selbst oder seinen gesetzlichen Vertreter richtet.[19] Schließlich darf der Arbeitnehmer gegenüber der außenstehenden Stelle nicht wissentlich unwahre oder leichtfertig falsche Angaben machen. Der Arbeitnehmer muss selbst präzise Angaben machen und die Vorwürfe mit Fakten belegen, damit diese in ihrer Substanz überprüft werden können.

Dies war möglicherweise bei Frau Heinisch in dem eingangs geschilderten Fall ein gewisses Problem: Die Anzeige gegenüber der Staatsanwaltschaft mit dem Verdacht auf Abrechnungsbetrug konnte Frau Heinisch nicht substantiieren – weder im Arbeitsgerichtsprozess noch gegenüber der Staatsanwaltschaft, weshalb das Ermittlungsverfahren auch eingestellt wurde.[20]

c) Keine grundlegende Neubewertung aufgrund des EGMR-Urteils vom 21.7.2011 in der Rechtssache „Heinisch“

Die geschilderten Grundsätze dieser Rechtsprechung bedürfen aus meiner Sicht auch nicht der Neuorientierung auf Grund des eingangs geschilderten „Heinisch“-Urteils des EGMR. Der EGMR hat hier nicht die abstrakten Grundsätze der BAG-Rechtsprechung in Zweifel gezogen, sondern lediglich die Subsumtion.[21] Dies ergibt sich aus der Argumentation des EGMR: Der EGMR betont, dass der Arbeitnehmer gegenüber dem Arbeitgeber zur Loyalität und Vertraulichkeit verpflichtet ist und leitet hieraus den Grundsatz des Vorrangs der innerbetrieblichen Klärung ab; nur als letztes Mittel dürfe der Arbeitnehmer sich mit den Informationen an die Öffentlichkeit wenden.[22] Der EGMR akzeptiert also die wesentlichen Grundsätze der BAG-Rechtsprechung. Er hält primär den Wert der Meinungsfreiheit durch die innerstaatlichen Gerichte für untergewichtet; diese hatte in der Tat in der Rechtsprechung bislang kaum eine Rolle gespielt.[23]

Zu dieser Einschätzung gelangt der EGMR aufgrund von zwei Gesichtspunkten des konkreten Falles: Zum einen bestand in diesem Fall ein besonderes öffentliches Interesse an der Aufdeckung von Missständen im Pflegebereich. Zum anderen stellte der EGMR bei der Bewertung der Leichtfertigkeit der Anzeigenerstattung wesentlich höhere Anforderungen als die Vorinstanzen des Ausgangsfalls.[24] Der EGMR dürfte daher insgesamt „Whistleblowern“ freundlicher gesonnen sein als dies jedenfalls die arbeitsgerichtlichen Instanzen des Ausgangsfalls waren.

d) Sanktionen

Hier gibt es reichlich Fallmaterial aus der Rechtsprechung. Die Rechtsprechung hält eine außerordentliche Kündigung wegen der Erstattung einer Strafanzeige gegen den Arbeitgeber grundsätzlich für möglich. Die Erstattung der Strafanzeige ist also „an sich“ geeignet, einen wichtigen Grund für eine außerordentliche Kündigung darzustellen, wenn und soweit der Arbeitnehmer dadurch wie skizziert gegen seine Rücksichtnahmepflicht aus § 241 Abs. 2 BGB verstoßen hat. Dies kann insbesondere der Fall sein, wenn der Arbeitnehmer den Grundsatz der vorrangigen innerbetrieblichen Abhilfe nicht beachtet hat oder wissentlich oder leichtfertig unzutreffende Angaben macht.

Daran hat auch das skizzierte Urteil des EGMR vom 21.7.2011 nichts geändert. Allerdings muss die Rechtsprechung nun in der Interessenabwägung stärker die beiden Aspekte berücksichtigen, die nach Auffassung des EGMR bislang zu kurz gekommen sind: Die Bedeutung der Meinungsäußerungsfreiheit und das öffentliche Interesse an Informationen über Missstände in bestimmten Wirtschaftszweigen, welche von allgemeiner Bedeutung sind – etwa Bereiche der Medizin und Pflege, Lebensmittelproduktion usw. Hier eine Grenze zu ziehen dürfte allerdings nicht einfach sein. Je nach Einzelfall kommen ferner ordentliche verhaltensbedingte Kündigung oder auch eine Abmahnung in Betracht. Außerhalb des Anwendungsbereichs des KSchG gilt natürlich wie stets das Maßregelungsverbot des § 612a BGB.

e) § 5 Nr. 2 GeschGehG

§ 5 Nr. 2 GeschGehG lautet: „Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses fällt nicht unter die Verbote des § 4, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere 2. zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, dass allgemeine öffentliche Interesse zu schützen.“ Die Vorschrift ist mit dem Geschäftsgeheimnisgesetz am 18.4.2019 in Kraft getreten und geht auf die fast gleichlautende Vorschrift des Art. 5 lit. b RL 2016/943/EU zurück. Es gibt noch keine Anwendungserfahrungen mit dieser Vorschrift. Deshalb ist unklar, ob die vorstehend skizzierten Grundsätze hierdurch verändert werden. Das Schrifttum ist wie stets bei solchen Fragen gespalten,[25] überwiegend wird dies jedoch abgelehnt und in der Vorschrift nur eine Bestätigung der bisherigen Rechtsgrundsätze gesehen.[26]

III. Datenschutzrechtliche Problematik von Hinweisgebersystemen

Externes Whistleblowing ist für Unternehmen unangenehm bis gefährlich: Externes Whistleblowing kann Rufschädigung, schlechte Presse bis hin zu straf- oder bußgeldrechtlicher Verfolgung verursachen. Unternehmen haben daher ein erhebliches Interesse daran, externes Whistleblowing zu vermeiden. Man kann es vermeiden, indem man internes Whistleblowing ermöglicht. Auf diesen Zusammenhang habe ich schon eingangs hingewiesen. Die Einrichtung von internen Hinweisgebersystemen ist aus dieser Perspektive folgerichtig. Hierdurch verbleibt unternehmensinternes Wissen über Regelverstöße im Internum des Unternehmens und wird vielfach überhaupt erst nutzbar.

Unter einem solchen Hinweisgebersystem versteht man im Allgemeinen folgendes: Das Unternehmen stellt eine Einrichtung zur Verfügung, die Arbeitnehmer benutzen können/sollen, um über möglicherweise rechtswidrige/verpönte Vorkommnisse im Betrieb berichten zu können. Spezifische gesetzliche Vorgaben oder Regelungen hierfür gibt es in Deutschland nur im Bereich Banken, Versicherungen und Finanzdienstleistungen (§ 4d FinDAG, § 29 VAG, § 25a Abs. 1 S. 6 Nr. 3 KWG, Art. 32 VO [EU] Nr. 596/2014, Art. 28 VO [EU] Nr. 1286/2014). Die Umsetzung der Hinweisgeberrichtlinie der EU wird dies verändern, weil danach Unternehmen mit mehr als 50 Arbeitnehmer ein derartiges System einrichten müssen.

Ansätze gesetzlicher Regelungen im Hinblick auf die Einrichtung von Beschwerdestellen enthalten § 13 AGG und § 84 BetrVG. Hier geht es aber zumeist um die Beschwerde in eigenen Angelegenheiten. Demgegenüber dient ein Hinweisgebersystem dazu, Informationen im Unternehmen über Regelverstöße zu sammeln und zu kanalisieren, damit diese das Unternehmen abstellen kann. Im Folgenden werde ich die datenschutzrechtlichen Implikationen solcher Hinweisgebersysteme behandeln.

1. Grundlegende Weichenstellungen bei der Etablierung von Hinweisgebersystemen

a) Interne oder externe Stelle?

Etabliert man ein solches System, muss man sich zunächst fragen, ob man eine interne oder eine externe Stelle mit der Aufnahme und Untersuchung der Hinweise betrauen möchte. Handelt es sich um eine interne Stelle, muss durch Verfahrensregeln gesichert sein, dass diese unabhängig ist und die übermittelten Informationen nicht an andere Personen, etwa Vorgesetzte oder die Personalabteilung, gelangen. Ohne strikte Vertraulichkeit wird das Hinweisgebersystem unter den Arbeitnehmern nicht die gewünschte Akzeptanz erlangen, was die Effizienz des Systems entscheidend schwächt. Allerdings kann ein Unternehmen strikte Vertraulichkeit gegenüber staatlichen Behörden, die über Zwangsmittel verfügen, wie etwa die Staatsanwaltschaft, ohnehin nicht garantieren. Das Erfordernis strikter Vertraulichkeit bezieht sich zunächst also auf den unternehmensinternen Bereich.

Bei einer externen Stelle stellt sich die Frage, wer im Sinne des Datenschutzrechts Verantwortlicher ist. Bei Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO bleibt dies der Arbeitgeber bzw. das Unternehmen, um dessen Hinweisgebersystem es geht. Auftragsdatenverarbeitung liegt nur vor, wenn der Arbeitgeber dem Drittunternehmen enge Vorgaben macht und die Parteien einen entsprechenden Vertrag nach Maßgabe von Art. 28 DS-GVO geschlossen haben.

Organisiert das Drittunternehmen – der externe Dienstleister – dagegen das Hinweisgebersystem unabhängig und in Eigenverantwortung, führt es etwa eigene Untersuchungen durch, dann ist der externe Dienstleister selbst für die Datenverarbeitung verantwortlich und damit ebenso wie der Arbeitgeber selbst verantwortliche Stelle im Sinne des Datenschutzrechts. In diesem Fall aber muss der externe Dienstleister wie der Arbeitgeber selbst die anwendbaren Rechtsgrundlagen

18 Vgl. BAG 3.7.2003 – NJW 2004, 1547; BVerfG 2.7.2001 – AP BGB § 626 Nr. 170.
19 BAG 7.12.2006 – 2 AZR 400/05 – NZA 2007, 502.
20 Siehe die Angaben bei LAG Berlin 28.3.2006 – 7 Sa 1884/05 – LAGE BGB 2002 § 626 Nr. 7b (unter 2.1.2.1.).
21 Ebenso die Einschätzung von *Schlachter*, RdA 2012, 108, 112.
22 EGMR 21.7.2011 – 28274/08 – NJW 2011, 3501, 3503 Rn. 65.
23 Siehe aber beispielsweise BVerfG 2.7.2001 – 1 BvR 2049/00 – AP Nr. 170 zu § 626 BGB.
24 Vgl. *Schlachter*, RdA 2012, 108, 112.
25 Überblick m.w.N. bei *Schubert*, in *Franzen/Gallner/Oetker* (Hrsg.), Kommentar zum europäischen Arbeitsrecht, 2. Aufl. 2018, Art. 5 RL 2016/943/EU Rn. 13.
26 Siehe etwa *Schmitt*, RdA 2017, 365, 371 f.

der Datenerhebung und -verarbeitung – Art. 6 DS-GVO bzw. § 26 BDSG – beachten. In der Literatur wird teilweise in Zweifel gezogen, dass deren Voraussetzungen vorliegen, weil der externe Dienstleister keinen eigenen arbeitsvertraglichen Verpflichtungen gegenüber den Arbeitnehmern unterliegt.[27] In diese Richtung tendierte auch die Arbeitsgruppe zu Art. 29 RL 95/46/EG.[28] Andererseits hält die Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises eine externe Untersuchungsstelle unter Umständen für vorteilhaft, weil die Hemmschwelle erhöht werde, Hinweise zu geben, und daher das Missbrauchsrisiko sinke.[29]

b) Anonymität des Hinweisgebers

Ferner stellt sich die weitere Grundfrage, ob der Hinweisgeber anonym bleiben kann oder seine Identität gegenüber dem Hinweisgebersystem offenlegen muss. Für eine anonyme Nutzbarkeit spricht die größere Akzeptanz des Verfahrens, weil ein Hinweisgeber nicht mit negativen Konsequenzen an seinem Arbeitsplatz rechnen muss. Dem steht das Interesse des potentiell belasteten betroffenen Arbeitnehmers gegenüber. Er muss sich verteidigen können, was für die Offenlegung der über ihn erhobenen Daten einschließlich der Quelle des Informanten spricht. Außerdem kann ein anonymes Hinweisgebersystem zu Denunziationen und unberechtigten Vorwürfen einladen, weil der anonyme Hinweisgeber weitgehend risikolos agiert. Dies kann einer Kultur des Misstrauens im Unternehmen Vorschub leisten. Aus diesen Gründen spricht sich die Arbeitsgruppe zu Art. 29 RL 95/46/EG dafür aus, die anonyme Nutzung eines Hinweisgebersystems nur subsidiär und komplementär zur offenen Nutzung zuzulassen, und setzt demgegenüber auf strikte Vertraulichkeit.[30]

2. Erhebung, Verarbeitung oder sonstige Nutzung personenbezogener Daten

a) Personenbezogene Daten

Datenschutzrecht ist nur anwendbar, wenn der Verantwortliche, regelmäßig der Arbeitgeber, personenbezogene Daten erhebt. Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare Person (betroffene Person) beziehen (Art. 4 Nr. 1 DS-GVO). Das Hinweisgebersystem kann nun vorsehen, dass überhaupt keine Namen genannt werden sollen – dass also vollständige Anonymität gewährleistet ist. Damit würde man die Anwendung des Datenschutzrechts von vornherein vermeiden. Allerdings wäre ein solches System wenig wirksam, da ohne Nennung von „Ross und Reiter" Regelverstöße kaum aufgeklärt werden können. Außerdem wird man rein faktisch kaum unterbinden können, dass personenbezogene Daten bei der Nutzung von Hinweisgebersystemen dann doch übertragen werden. Mit der Einrichtung eines Hinweisgebersystems ist daher realistischerweise regelmäßig die Übertragung personenbezogener Daten verbunden. Das Datenschutzrecht ist daher grundsätzlich einschlägig.

b) Erheben von Daten

Das Erheben von Daten wird in der DS-GVO nicht näher definiert. Man verstand bislang darunter das Beschaffen von Daten über den Betroffenen. Erforderlich ist danach ein zielgerichtetes Handeln des Verantwortlichen. Keine Datenerhebung durch den Arbeitgeber liegt daher vor, wenn er ohne eigenes Zutun Daten erhält, etwa durch eine unverlangte Mitteilung. Das bloße Vorhalten von herkömmlichen Empfangseinrichtungen, wie Briefkasten, Faxgerät, E-Mail-Accounts oder Websites mit Eingabemöglichkeit ist keine Datenerhebung.[31] Ein Hinweisgebersystem beschränkt sich aber nicht auf das Vorhalten einer solchen Empfangseinrichtung. Vielmehr werden die Arbeitnehmer aufgefordert oder gar verpflichtet, Hinweise über Regelverstöße ausschließlich in dieses System einzuspeisen. Damit etabliert der Arbeitgeber eine Einrichtung, die dem zielgerichteten Beschaffen von Daten dient. Richtet der Arbeitgeber also ein Hinweisgebersystem ein, bei dem Angaben über bestimmte oder bestimmbare Arbeitnehmer und deren Verhalten gemacht werden sollen, erhebt der Arbeitgeber somit personenbezogene Daten und befindet sich grundsätzlich im Anwendungsbereich der DS-GVO.

c) Sonstige Datenverarbeitung

Über diese Ersterhebung hinaus finden in einem Hinweisgebersystem weitere Datenerhebungen und –verarbeitungen statt. Nachfragen der Untersuchungsstelle auf die Erstinformation durch den Hinweisgeber hin erfüllt unproblematisch den Tatbestand der Datenerhebung. Ferner werden die erhobenen Daten im Rahmen der weiteren Untersuchung eines Hinweises gespeichert und in vielfältiger Weise genutzt. Die Aufgreifkriterien des Datenschutzrechts sind also spätestens dann eröffnet.

3. Datenschutzrechtlicher Erlaubnistatbestand (Art. 6 DS-GVO)

Nach Art. 6 DS-GVO bedarf die Verarbeitung personenbezogener Daten der betroffenen Person einer datenschutzrechtlichen Erlaubnis.

a) Einwilligung

Auf eine Einwilligung des betroffenen Arbeitnehmers kann ein Hinweisgebersystem nicht gestützt werden. Eine Einwilligung im Vorhinein ohne konkrete Betroffenheit – etwa als Zusatzvereinbarung beim Abschluss des Arbeitsvertrags – scheitert daran, dass der Arbeitnehmer die über ihn in einem Hinweisgebersystem zu erhebenden Daten im Vorhinein überhaupt nicht überblicken kann. Damit dürfte zweifelhaft sein, ob eine solche Einwilligung auf der „freien Entscheidung" des Betroffenen beruht, wie dies Art. 4 Nr. 11 DS-GVO verlangt.[32] Eine Einwilligung erst dann einzuholen, wenn konkrete Verdachtsmomente gegen den betroffenen Arbeitnehmer bestehen, kommt regelmäßig zu spät und ist überdies offenkundig unpraktikabel.

b) Betriebsvereinbarung

Eine Betriebsvereinbarung kann grundsätzlich tauglicher datenschutzrechtlicher Erlaubnistatbestand sein. Dies hat das BAG in einer bereits lange zurückliegenden Entscheidung festgestellt.[33] Dasselbe gilt unter der DS-GVO nach Art. 88 DS-GVO. Dies stellt eine Öffnungsklausel für die Mitgliedstaaten dar, den Datenschutz im Beschäftigungskontext weitgehend eigenständig zu regeln. Art. 88 Abs. 1 DS-GVO nennt ausdrücklich auch Kollektivvereinbarungen, womit vor allem Betriebsvereinbarungen gemeint sind. Allerdings ist derzeit noch nicht vollständig geklärt, wie weit diese Öffnungsklausel des Art. 88 DS-GVO reicht. Aus diesem Grund scheint es mir nicht empfehlenswert zu sein, ein Hinweisgebersystem datenschutzrechtlich ausschließlich auf eine Betriebsvereinbarung zu stützen.

c) Rechtspflicht zur Schaffung eines Hinweisgebersystems

Statuiert eine Rechtsvorschrift eine Rechtspflicht zur Schaffung eines Hinweisgebersystems, stellt dies eine Erlaubnisnorm im Sinne von Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO dar. Danach ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist. Nach Art. 6 Abs. 3 DS-GVO muss sich die Rechtsgrundlage hierfür aus Unionsrecht oder dem Recht der Mitgliedstaaten ergeben und die Zwecke der Verarbeitung festlegen.

In Deutschland gibt es solche Rechtsvorschriften – von Regelungen im Bereich der Banken, Versicherungen und Finanzdienstleistungen abgesehen – bislang nicht. Dies wird sich ändern, wenn die Hinweisgeberrichtlinie der EU in deutsches Recht umgesetzt wird. Denn diese schreibt vor, dass juristische Personen, die 50 und mehr Arbeitnehmer beschäftigen, ein Hinweisgebersystem etablieren müssen.

d) Art. 88 DS-GVO bzw. § 26 BDSG

Ob die arbeitsrechtlichen Erlaubnistatbestände der Art. 88 DS-GVO und § 26 BDSG Anwendung finden können, hängt von der Reichweite der Öffnungsklausel in Art. 88 DS-GVO ab. Art. 88 Abs. 1 DS-GVO nennt insoweit auch die „Planung und Organisation der Arbeit". Darunter wird man Hinweisgebersysteme subsumieren können.[34] Wenn man dem folgt, ist die deutsche Umsetzungsnorm des § 26 BDSG anwendbar.[35]

Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses oder zur Erfüllung von gesetzlichen Pflichten erforderlich ist. Dies wird man im Hinblick auf Hinweisgebersysteme grundsätzlich bejahen können, vor allem bei Arbeitgebern, welche zur Etablierung eines solchen Systems verpflichtet sind.

4. Interessengerechte Ausgestaltung des Hinweisgebersystems

Die konkrete Ausgestaltung des Hinweisgebersystems muss allerdings „erforderlich" im Sinne des § 26 Abs. 1 BDSG sein. Dieser „Erforderlichkeitsgrundsatz" wird von der Rechtsprechung im Sinne eines Verhältnismäßigkeitsgrundsatzes verstanden. Das Hinweisgebersystem muss so ausgestaltet sein, dass die berechtigten Interessen der betroffenen Person und des Verantwortlichen, des Arbeitgebers, berücksichtigt und in einen angemessenen Ausgleich gebracht werden. Im Vordergrund steht der Schutz der berechtigten Interessen der betroffenen Person.

a) Schutz der berechtigten Interessen des Betroffenen

Den berechtigten Interessen des Betroffenen muss Rechnung getragen werden dadurch, dass das Hinweisgebersystem Vorkehrungen gegen unberechtigte Anschuldigungen trifft. Diese Anforderung spricht zunächst gegen die Möglichkeit anonymer Anzeigen. Betroffene können sich gegen anonyme Vorwürfe nicht so gut wehren. Die Anonymisierung erleichtert das Vorbringen unberechtigter Vorwürfe ungemein;[36] der Hinweisgeber trägt kaum noch eigene Risiken. Andererseits kann es durchaus Situationen geben, in denen die Möglichkeit anonymisierter Hinweise angebracht erscheint. Insgesamt dürfte ein System vorzugswürdig sein, welches anonyme und offene Anzeigen gleichermaßen zulässt.[37] Offenbart der Hinweisgeber in dieser Situation seinen Klarnamen, liegt darin eine Einwilligung in die weitere Datenverarbeitung dieser

27 *Breinlinger/Krader*, RDV 2006, 60, 66.
28 Vgl. Stellungnahme 1/2006 der Artikel 29 Datenschutz Arbeitsgruppe vom 1.2.2006 über die Anwendung von EU-Datenschutzvorschriften hinsichtlich Hinweisgebersystemen, S. 15.
29 Ebenso Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz" des Düsseldorfer Kreises „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", April 2007, S. 7; ähnlich Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", November 2018, S. 13.
30 Stellungnahme 1/2006 der Artikel 29 Datenschutz Arbeitsgruppe vom 1.2.2006 über die Anwendung von EU-Datenschutzvorschriften hinsichtlich Hinweisgebersystemen, S. 11.
31 *Dammann*, in: *Simitis* (Hrsg.), BDSG, 7. Aufl. 2011, § 3 Rn. 104.
32 Ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", November 2018, S. 7.
33 BAG 27.5.1986 – DB 1986, 280.
34 So *Selk*, in: *Ehmann/Selmayr*, DS-GVO, 2. Aufl. 2019, Art. 88 DS-GVO Rn. 112.
35 Unklar Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, November 2018, S. 4 einerseits und S. 6 andererseits. Die DSK hält jedenfalls Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO für einschlägig, weil die berechtigten Interessen des Arbeitgebers überwiegen, aaO., S. 5 f.
36 Stellungnahme 1/2006 der Artikel 29 Datenschutz Arbeitsgruppe vom 1.2.2006 über die Anwendung von EU-Datenschutzvorschriften hinsichtlich Hinweisgebersystemen, S. 11; ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", November 2018, S. 8.
37 Stellungnahme 1/2006 der Artikel 29 Datenschutz Arbeitsgruppe vom 1.2.2006 über die Anwendung von EU-Datenschutzvorschriften hinsichtlich Hinweisgebersystemen, S. 11; für regelmäßig anonyme Verfahren Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz", November 2018, S. 9.

Angaben, wenn das Unternehmen die formalen Erfordernisse des Art. 7 DS-GVO beachtet – insbesondere die Information über die jederzeitige Widerruflichkeit der Einwilligung.[38]

Ferner muss das Hinweisgebersystem strikte Vertraulichkeit garantieren. Unternehmensinterne Untersuchungsstellen müssen daher unabhängig sein. Es muss sichergestellt sein, dass andere Stellen des Unternehmens, etwa die Personalabteilung oder die betroffene Fachabteilung keine Informationen erhalten. Außerdem muss die Untersuchungsstelle den Sachverhalt in eigener Verantwortung zuerst ausermitteln können und nach Abschluss den Vorgang einstellen oder vertraulich je nach Bedeutung an Geschäftsführung oder Bereichsleitung übermitteln.

Darüber hinaus kann verlangt werden, dass vorgetragene Angaben nur aufgenommen und untersucht werden, wenn diese plausibel sind und auf konkreten Tatsachen beruhen. Dies würde nebenbei bemerkt die Anforderungen des § 26 Abs. 1 S. 2 BDSG erfüllen. Diese Voraussetzung würde aber das Instrument möglicherweise entwerten.

Ferner kann das Hinweisgebersystem den Hinweisgeber darauf aufmerksam machen, dass falsche Angaben unter Umständen strafbar sind – etwa nach § 186 StGB oder § 187 StGB (Üble Nachrede oder Verleumdung). Je nach Ausgestaltung kann dies potentielle Hinweisgeber aber abschrecken, das System zu nutzen. Letztlich kann man hierdurch die Wirksamkeit des Systems unterminieren.

Die Interessen des Betroffenen werden weiter durch eine Pflicht zu dessen alsbaldiger Anhörung geschützt. Dies kann allerdings mit dem Aufklärungsinteresse kollidieren. Daher sollte der Betroffene erst dann angehört werden müssen, wenn Verdunkelungsgefahr ausgeschlossen werden kann.[39]

Die Interessen des Betroffenen kann man ferner dadurch schützen, dass das Hinweisgebersystem den datenschutzrechtlichen Grundsätzen der Datenvermeidung und -sparsamkeit genügt. Ferner sollten Vorkehrungen existieren, damit personenbezogene Daten gegebenenfalls gelöscht, berichtigt oder gesperrt werden, um damit den Erfordernissen der Art. 16 ff. DS-GVO zu genügen.

b) Erhebliche Interessen des Arbeitgebers

Die Datenverarbeitung lässt sich umso leichter rechtfertigen, je gewichtiger die Interessen des Verantwortlichen – also des Arbeitgebers – an der Datenerhebung und -nutzung sind. Daher erscheint erwägenswert, die im Hinweisgebersystem anzugebenden Verfehlungen auf wichtige Problemkreise zu beschränken, etwa auf den Verdacht von Straftaten und erheblichen Pflichtverletzungen oder auf Regelverstöße, welche unter Compliance-Gesichtspunkten erheblich sind – etwa aufgrund von Vorschriften des WpHG oder aufgrund von Vorgaben der US-amerikanischen Börsenaufsicht. Allerdings kann dies kontraproduktiv wirken. Diese Voraussetzungen können Arbeitnehmer davon abhalten, überhaupt Angaben zu machen. Außerdem lässt sich die Dimension und Bedeutung eines Hinweises am Anfang oft überhaupt nicht einschätzen. Dies dürfte dafür sprechen, ein Hinweisgebersystem doch für alle Pflichtverletzungen zu öffnen.

Denkbar ist ferner, die anzuzeigenden Verfehlungen auf bestimmte Arten von Mitarbeitern zu beschränken, beispielsweise Führungskräfte. Dagegen kann man allerdings einwenden, dass der Arbeitgeber generell ein Interesse hat, Regelverstöße von Gewicht in seinem Unternehmen aufzuklären, um sie abstellen zu können. Solche Regelverstöße können grundsätzlich von jedem Mitarbeiter und nicht nur von Führungskräften begangen werden. Daher empfiehlt sich die Begrenzung auf bestimmte Mitarbeiterkategorien nicht unbedingt.

5. Informationspflichten nach Art. 13 und 14 DS-GVO

Art. 13 und 14 DS-GVO verpflichten den Verantwortlichen, die betroffene Person über die Datenverarbeitung nach näherer Maßgabe dieser Vorschriften zu informieren. Art. 13 DS-GVO erfasst dabei den Fall, dass die Daten direkt bei der betroffenen Person erhoben werden, also mit deren Wissen oder Mitwirkung, während Art. 14 DS-GVO den anderen Fall betrifft, wenn also Daten ohne Wissen oder Mitwirkung der betroffenen Person erhoben werden. Vorliegend ist daher Art. 14 DS-GVO einschlägig. Deshalb kann man den Dispenstatbestand des Art. 14 Abs. 5 lit. b DS-GVO auf Hinweisgebersysteme anwenden.[40] Danach kann die Information unterbleiben, wenn die Informationserteilung die Ziele der Verarbeitung ernsthaft beeinträchtigen würde. Daher wird man im Rahmen von Hinweisgebersystemen von einer Information der betroffenen Person absehen können, solange noch eine Verdunkelungsgefahr besteht.

6. Auskunftsrecht nach Art. 15 DS-GVO

Auf das Auskunftsrecht der betroffenen Person nach Art. 15 DS-GVO ist Art. 14 Abs. 5 lit. b DS-GVO allerdings nicht anwendbar. In § 34 Abs. 1 BDSG ist das Auskunftsrecht jedenfalls für nicht öffentliche Stellen ebenfalls nicht weiter eingeschränkt, weil der Verweis in § 34 Abs. 1 S. 1 Nr. 1 BDSG auf § 33 Abs. 1 BDSG die hier relevante Vorschrift des § 33 Abs. 1 Nr. 2a BDSG gerade ausnimmt. Danach besteht eine Informationspflicht nicht, wenn die Auskunft die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde (§ 33 Abs. 1 Nr. 2a BDSG).

Allerdings wird man in solchen Fällen § 29 Abs. 1 S. 2 BDSG anwenden können. Danach besteht das Auskunftsrecht nach Art. 15 DS-GVO nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen eines Dritten, geheim gehalten werden müssen.[41]

38 Ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“, November 2018, S. 9.
39 Stellungnahme 1/2006 der Artikel 29 Datenschutz Arbeitsgruppe vom 1.2.2006 über die Anwendung von EU-Datenschutzvorschriften auf hinsichtlich Hinweisgebersystemen, S. 13.

40 Ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“, November 2018, S. 10.

IV. Fazit

Gestatten Sie mir ein kurzes Fazit meiner Überlegungen: Hinweisgebersysteme sind geeignet, im Unternehmen vorhandene Informationen über Regelverstöße für das Unternehmen nutzbar zu machen. Hinweisgebersysteme können daher internes „Whistleblowing“ kanalisieren und mithelfen, dass es gar nicht zu „externem Whistleblowing“ kommt. Fälle wie derjenige der Altenpflegerin Frau Heinisch, der bis zum Europäischen Gerichtshof für Menschenrechte gelangt ist, sollten Unternehmen im eigenen Interesse vermeiden. Hinweisgebersysteme können grundsätzlich datenschutzkonform ausgestaltet werden, wenn die berechtigten Interessen der betroffenen Personen ausreichend berücksichtigt werden.[42] Dies bedeutet insbesondere: anonyme Hinweise sollten eher die Ausnahme und nicht den Regelfall darstellen. Die mit den Hinweisen befasste Untersuchungsstelle muss strikte Vertraulichkeit wahren, sie muss unabhängig sein und eigenständig den Sachverhalt ermitteln können. Der betroffene Arbeitnehmer muss über die Vorwürfe informiert und angehört werden, sobald eine Verdunkelungsgefahr nicht mehr besteht.

41 Ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“, November 2018, S. 11.
42 Ebenso Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Orientierungshilfe zu „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“, November 2018, S. 13.

Vortrag zur Veranstaltung
Prof. Dr. Klaus Ulrich Schmolke, LL.M. (NYU),
Friedrich-Alexander-Universität Erlangen-Nürnberg

Die neue EU-Richtlinie zum Whistleblowerschutz und ihre Umsetzung in Deutschland[1]

I. Thema

Am 23. Oktober 2019 wurde die Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, kurz: Whistleblower-Richtlinie von den Präsidenten des Rates und des Parlaments, unterzeichnet. Damit gilt bald ein europaweiter Mindestschutz für Whistleblower, die auf Verstöße gegen bestimmte Normen des EU-Rechts hinweisen.[2] Die Mitgliedstaaten haben bis Ende 2021 Zeit, diese Vorgaben umzusetzen. Gewisse Entscheidungen über Reichweite und Umfang des Hinweisgeberschutzes hat die Richtlinie aber auch ausdrücklich in die Hände der Mitgliedstaaten gelegt. Angesichts des mindestharmonisierenden Charakters der Richtlinie bleibt es dem deutschen Gesetzgeber zudem unbenommen, über den Schutzstandard der Richtlinie hinauszugehen.[3] Interessenverbände wie das *Whistleblower Netzwerk* und *Transparency International Deutschland* haben dem deutschen Gesetzgeber daher gleich mit Verabschiedung der Richtlinie auf EU-Ebene Umsetzungsvorschläge unterbreitet.[4] Der politische Kampf um die Reichweite des Whistleblowerschutzes geht damit für Deutschland in eine neue Runde.

II. Ein Blick zurück – Der Kampf um die Richtlinie

Treibende Kraft für einen europaweiten Hinweisgeberschutz war nicht die Kommission, sondern das Europäische Parlament. Nachdem das Unionsrecht in den vergangenen Jahren bereits in einigen Rechtsgebieten spezielle Bestimmungen zum Hinweisgeberschutz getroffen hatte, sah das Parlament die Zeit für eine umfassendere Regelung gekommen. In zwei Entschließungen aus dem Jahr 2017 drängte es die Kommission, einen „horizontalen Gesetzgebungsvorschlag zur Schaffung eines umfassenden gemeinsamen Rechtsrahmens vorzulegen, der Hinweisgebern in der EU ein hohes Maß an Schutz im öffentlichen und privaten Sektor […] gewährleistet".[5] Im April 2018 legte die Kommission dann ihren Richtlinienvorschlag vor.[6] Dem Parlament ging dieser Vorschlag indes nicht weit genug. Der Bericht des federführenden Rechtsausschusses sah in seinem Entwurf einer legislativen Entschließung des Parlaments daher zahlreiche Änderungen zugunsten potenzieller Whistleblower vor.[7] Dies betraf etwa die Ausweitung des personalen Anwendungsbereichs der Schutzvorschriften auf „Mittler", die zur Meldung einen Beitrag leisten oder den Hinweisgeber hierbei unterstützen, den ausdrücklichen Schutz auch anonym meldender (und später enttarnter) Hinweisgeber, vor allem aber die Aufgabe der Stufenfolge (1) interne Meldung, (2) externe Meldung an die zuständige Behörde und (3) Bekanntmachung gegenüber der Öffentlichkeit als Voraussetzung des Hinweisgeberschutzes.[8] Der revidierte Richtlinienvorschlag der Ratspräsidentschaft von Ende 2018 hielt allerdings zunächst noch am grundsätzlichen Vorrang der internen Meldung fest.[9] Der politische Druck war indes zu groß. Im Trilogverfahren räumte der Rat seine Position und stimmte der Anwendung der Schutzbestimmungen der Richtlinie auch bei direkter Meldung an die Aufsichtsbehörden zu.[10] Nach der politischen Einigung zwischen Rat und Parlament stimmte das Parlament der Richtlinie am 16. April 2019 und damit noch vor der Europawahl in der ausgehandelten Fassung zu.[11] Jedoch zeigte sich bald, dass die rege Gesetzgebungstätigkeit kurz vor Ende der Legislaturperiode auf Kosten der Sorgfalt gegangen war. Die Whistleblower-Richtlinie musste daher noch einmal ins Berichtigungsverfahren[12], so dass der Rat erst am 7. Oktober 2019 ebenfalls zustimmen konnte.[13]

III. Die neue Richtlinie als (vorläufiges) Ergebnis

Im Folgenden sollen die wichtigsten Regelungsinhalte der neuen Richtlinie kurz vorgestellt werden (1.). Besonderes Augenmerk gilt dabei den Umsetzungsspielräumen der Mitgliedstaaten (2.).

1. Wesentliche Inhalte der Richtlinie – Determinanten für den Umsetzungsgesetzgeber

Sachlicher Anwendungsbereich: Die Richtlinie erfasst die Meldung von Verstößen gegen die unterschiedlichsten Vorschriften des EU-Rechts. Dies betrifft beispielsweise das öffentliche Auftragswesen, Finanzdienstleistungen, Produktsicherheit, Umweltschutz oder Verbraucherschutz.[14] Dieser breite Anwendungsbereich macht den „horizontalen" Charakter der Richtlinie aus.

Personaler Anwendungsbereich: Die Richtlinie zieht den Kreis der geschützten Personen weit (siehe Art. 4 WBRL).[15] Zwar werden „zuallererst" Arbeitnehmer i.S.d. Art. 45 Abs. 1 AEUV geschützt, was auch Beamte und andere im öffentlichen Sektor arbeitende Personen einschließt.[16] Der Schutz reicht aber deutlich weiter. Dem liegt der zutreffende Gedanke zugrunde, dass für eine effektive Rechtsdurchsetzung qua Whistleblowing möglichst alle Personengruppen geschützt werden sollten, die „aufgrund ihrer beruflichen Tätigkeit, unabhängig von der Art dieser Tätigkeit […], privilegierten Zugang zu Information über Verstöße, deren Meldung im öffentlichen Interessen liegt, haben und die im Falle einer solchen Meldung Repressalien erleiden könnten".[17] Keine Rolle spielt dabei, welche Motive den Hinweisgeber zur Meldung veranlasst haben.[18] Auf Betreiben des Parlaments werden neben dem Hinweisgeber selbst nunmehr auch dritte Personen geschützt, die den Hinweisgeber bei seiner Meldung unterstützt haben, oder sonst besonders gefährdet sind, Opfer von Repressalien zu werden.[19]

Voraussetzungen für den Hinweisgeberschutz/Meldefolge: Nach Art. 6 WBRL hat Anspruch auf Schutz, wer mit hinreichendem Grund davon ausgehen durfte, dass die gemeldete Information zutrifft und einen Verstoß darstellt, der in den Anwendungsbereich der Richtlinie fällt. Der Hinweisgeber kann die Meldung nach seiner Wahl zunächst *intern*, das heißt an eine geeignete Stelle innerhalb der Organisation, melden oder sich sogleich *extern* an die zuständige Behörde wenden (Art. 6 Abs. 1 lit. b i.V.m. Art. 7 und 10 WBRL). Jedoch sollen sich die Mitgliedstaaten dafür einsetzen, dass die Meldung zunächst intern durchgeführt wird (Art. 7 Abs. 2 WBRL).[20] Legt der Hinweisgeber die Informationen über den vermeintlichen Verstoß offen, geht er also an die Öffentlichkeit (vgl. Art. 5 Nr. 5 WBRL), so hat er nur dann Anspruch auf den durch die Richtlinie gewährten Schutz, wenn er zunächst intern oder extern gemeldet hat, aber innerhalb der in der Richtlinie festgelegten Höchstfristen keine geeigneten Maßnahmen ergriffen worden sind, oder wenn er davon ausgehend durfte, dass der Verstoß eine „unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses" darstellen kann, oder dass im Falle einer externen Meldung Repressalien zu befürchten sind oder aufgrund der besonderen Umstände des Falles geringe Aussichten bestehen, dass wirksam gegen den Verstoß vorgegangen wird, etwa bei Kollusion zwischen dem Delinquenten und der Behörde (Art. 6 Abs. 1 lit. b i.V.m. Art. 15 Abs. 1 WBRL).[21]

1 Der vorliegende Text wurde am 15.11.2019 an der LMU München im Rahmen der Tagung „Whistleblowing in Deutschland – Zivilcourage oder Verrat? Hinweisgeberverhalten und rechtliche Regelung in Deutschland" gehalten. Eine deutliche erweiterte Fassung dieses Textes ist in Heft 1/2020 der NZG unter dem Titel „Die neue Whistleblower-Richtlinie ist da! Und nun?" erschienen.
2 Richtlinie (EU) 2019/1937 v. 23.10.2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABL. EU v. 26.11.2019, L305/17.
3 Siehe dazu noch unten unter IV.2. pr.
4 Siehe das für die beiden Verbände erstellte Papier von *Gerdemann*, Überlegungen zur nationalen Umsetzung der Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden („Whistleblowing-Richtlinie"), online: https://www.whistleblower-net.de/wp-content/uploads/2019/10/%C3%9Cberlegungen-zur-nationalen-Umsetzung-der-Whistleblowingrichtlinie.pdf.
5 Entschließung des Europäischen Parlaments v. 14.2.2017 zur Rolle von Informanten beim Schutz der finanziellen Interessen der EU (2016/2055(INI), online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0022+0+DOC+PDF+V0//DE, und Entschließung des Europäischen Parlaments vom 24.10.2017 zu legitimen Maßnahmen zum Schutz vor Hinweisgebern, die aus Gründen des öffentlichen Interesses vertrauliche Informationen über Unternehmen und öffentliche Einrichtungen offenlegen, 2016/2224(INI), online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0402+0+DOC+PDF+V0//DE.
6 *Kommission*, Vorschlag für eine Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, COM (2018) 218 final, 23.4.2018, online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018PC0218.
7 *Europäisches Parlament*, Entwurf eines Berichts des Rechtsausschusses (Berichterstatterin *Virginie Rozière*) über den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, 2.7.2018, 2018/0106(COD). Die Stellungnahme enthielt 65 Änderungsvorschläge. Diese sind durch weitere Eingaben auf stolze 577 angeschwollen, siehe dazu die unter http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=&reference=2018/0106(COD) abrufbaren Dokumente des Rechtsausschusses.
8 Siehe Entwurf einer legislativen Entschließung, online: https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2018/0398/P8_A(2018)0398_DE.pdf; zum vorausgehenden Entwurf der Berichterstatterin *Virginie Rozière* siehe bereits *Schmolke*, AG 2018, 769, 777 ff.
9 Siehe *Council of the EU* – Presidency, Proposal for a Directive on the protection of persons reporting on breaches of Union law, 10 December 2018, dort insb. Erwägungsgrund 23ter und Art. 2bis i.V.m. Art. 5bis, online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15178_2018_INIT&from=DE.
10 Siehe *Europäisches Parlament*, Pressemitteilung v. 12.3.2019, online: https://www.europarl.europa.eu/news/de/press-room/20190311IPR31055/whistleblower-erstmals-eu-weiter-schutz-fur-hinweisgeber.
11 Legislative Entschließung des Europäischen Parlaments vom 16.4.2019 zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, online: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0366_DE.html.
12 Für nähere Informationen zum Verfahrensgang siehe https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:52018PC0218.
13 Rat der EU, Vermerk v. 11.10.2019, online: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CONSIL:ST_13039_2019_INIT&from=EN.
14 Vgl. Erwägungsgrund 24 WBRL.
15 Siehe zur bereits großzügigen Regelung des Kommissionsvorschlags *Schmolke*, AG 2018, 769, 777.
16 Siehe Erwägungsgrund 38 WBRL.
17 Siehe Erwägungsgrund 37 S. 1 WBRL; zum Kommissionsvorschlag bereits *Schmolke*, AG 2018, 769, 777.
18 Siehe Erwägungsgrund 32 S. 5.
19 Siehe für Einzelheiten Art. 4 Abs. 4 und Art. 5 Nr. 8, 9, 11 WBRL.
20 Siehe dazu noch unten unter IV.2.6.
21 Siehe zur Offenlegung des Verstoßes auch die Ausführungen in den Erwägungsgründen 79 ff. WBRL, ferner die etwas kryptisch formulierte

Pflicht zur Einrichtung interner und externer Meldekanäle/ Verfahrensstandards: Die Richtlinie will Whistleblower nicht nur schützen, *falls* sie einen Verstoß melden, sondern auch eine effektive Meldeinfrastruktur für potenzielle Hinweisgeber gewährleisten. Daher werden die Mitgliedstaaten verpflichtet sicherzustellen, dass juristische Personen des privaten Sektors mit 50 oder mehr Arbeitnehmern sowie juristische Personen des öffentlichen Sektors Kanäle und Verfahren für interne Meldungen und daran anschließende Folgemaßnahmen einrichten (siehe Art. 8 WBRL).[22] Die einzurichtenden Verfahren haben gewisse Mindeststandards einzuhalten, welche insbesondere die Wahrung der Vertraulichkeit,[23] die Transparenz des Verfahrens und Rückmeldungen innerhalb angemessener Frist betreffen (Art. 9 WBRL). Ganz ähnliche Regelungen finden sich für die Einrichtung externer Meldeverfahren bei den zuständigen Behörden der Mitgliedstaaten (Art. 11 ff. WBRL).

Schutzmaßnahmen für den Hinweisgeber: Die Richtlinie gewährleistet den Schutz von Hinweisgebern, indem sie den Mitgliedstaaten aufgibt, Repressalien und deren Androhung zu verbieten (Art. 19 WBRL), die erforderlichen Maßnahmen zum Schutz vor gleichwohl angewandten Repressalien zu ergreifen (Art. 21 WBRL) sowie Zugang zu sog. unterstützenden Maßnahmen zu gewähren (Art. 20 WBRL). Art. 19 WBRL listet einige wichtige Beispiele für Repressalien auf, wie etwa Kündigung, Versagung einer Beförderung, Mobbing und Ausgrenzung, Diskriminierung, Rufschädigung, Blacklisting oder – besonders perfide – psychiatrische oder ärztliche Überweisungen. Auch hinsichtlich der erforderlichen Schutzmaßnahmen vor Repressalien führt die Richtlinie Beispiele auf, die von den Mitgliedstaaten jedenfalls einzuführen sind (siehe Art. 21 Abs. 2 bis 8 WBRL). So gilt etwa die für eine Meldung von Verstößen erforderliche Offenlegung von Informationen grundsätzlich nicht als Verletzung von Verschwiegenheits- und Geheimhaltungspflichten (Art. 21 Abs. 2 WBRL). Auch können die Hinweisgeber nicht wegen Verleumdung, Urheberrechtsverletzung, Verstoßes gegen Datenschutzvorschriften oder Offenlegung von Geschäftsgeheimnissen haftbar gemacht werden, sofern sie „hinreichenden Grund zu der Annahme hatten, dass die Meldung oder Offenlegung notwendig war", um den Verstoß aufzudecken (Art. 21 Abs. 7 WBRL). Ebenso wird der Hinweisgeber vor einer Haftung für die Beschaffung der gemeldeten Information geschützt, sofern diese Beschaffung „nicht als solche eine eigenständige Straftat" darstellt (Art. 21 Abs. 3 WBRL).[24] Ferner wird zugunsten des Hinweisgebers vermutet, dass eine erlittene Benachteiligung eine Repressalie für die Meldung oder Offenlegung des Verstoßes war (Art. 21 Abs. 5 WBRL).[25] Schließlich müssen die Mitgliedstaaten auch geeignete Abhilfemaßnahmen gegen Repressalien vorhalten (Art. 21 Abs. 6 WBRL) sowie für die Möglichkeit zur vollständigen Kompensation bereits erlittener Schäden sorgen (Art. 21 Abs. 8 WBRL).

Schutz der von der Meldung betroffenen Personen: Die Regelungen der Richtlinie zum Schutz der von der Meldung des Hinweisgebers betroffenen Personen nehmen sich demgegenüber bescheiden aus.[26] Art. 22 WBRL verweist zum einen auf die auch diesen Personen selbstverständlich zustehenden Verfahrensgrundrechte (Abs. 1) und trifft zum anderen Regelungen zum Schutz der Identität der von der Meldung betroffenen Person (Abs. 2 und 3). Ferner haben die Mitgliedstaaten wirksame, angemessene und abschreckende Sanktionen für Hinweisgeber festzulegen, die wissentlich falsche Informationen gemeldet oder offengelegt haben. In diesem Fall sind auch Maßnahmen zu Wiedergutmachung von Schäden vorzusehen, also insbesondere Schadensersatzansprüche (Art. 23 Abs. 2 WBRL).

2. Umsetzungsspielräume des nationalen Gesetzgebers

Neben den soeben skizzierten Vorgaben für den nationalen Gesetzgeber belässt die Richtlinie den Mitgliedstaaten auch erhebliche Gestaltungsspielräume, in denen sich der Kompromisscharakter des Rechtsakts deutlich zeigt. Diese Spielräume ergeben sich zunächst und vor allem daraus, dass die Richtlinie lediglich Mindeststandards für den Schutz von Hinweisgebern festlegt (siehe insb. Art. 1 WBRL),[27] über die der nationale Gesetzgeber hinausgehen kann.

Abgesehen von ihrem mindestharmonisierenden Charakter gewährt die Richtlinie den Mitgliedstaaten nicht selten Wahlrechte zur Ausgestaltung bestimmter Einzelregelungen des Hinweisgeberschutzregimes oder verweist auf nicht harmonisierte Regelungsbereiche. Schließlich enthält die Richtlinie zahlreiche unbestimmte Rechtsbegriffe, die der Konkretisierung bedürfen.[28] Nur beispielhaft sei hier auf folgende Bestimmungen hingewiesen:

— Art. 3 Abs. 2 bis 4 WBRL nimmt bestimmte Regelungskomplexe vollständig aus dem harmonisierten Bereich der Richtlinie heraus. Hierzu gehört namentlich die nationale Sicherheit, so dass Meldungen, die Verteidigungs- und Sicherheitsaspekte betreffen, nicht unter die Richtlinie fallen. Auch bleibt der nationale Schutz von Verschlusssachen aus Sicherheitsgründen unberührt.[29] Ein europäischer Fall „Snowden"[30] wäre von der Richtlinie daher nicht erfasst.

— Art. 6 Abs. 2 WBRL weist den Mitgliedstaaten die Entscheidung darüber zu, ob juristische Personen des privaten oder öffentlichen Sektors sowie zuständige Behörden als Adressaten interner und externer Meldungen zur Entgegennahme und Weiterverfolgung anonymer Hinweise verpflichtet sind.[31] Hiervon unberührt bleibt der zwingende Schutz zunächst anonym meldender, später aber enttarnter Hinweisgeber durch die Richtlinie.[32]

— Vom ursprünglich vorgesehenen Vorrang interner Meldung ist lediglich die Regelung in Art. 7 Abs. 2 WBRL übriggeblieben. Danach setzen sich die Mitgliedstaaten dafür ein, dass die Meldung über interne Meldekanäle gegenüber der Meldung über externe Meldekanäle in den Fällen bevorzugt wird, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien befürchtet. Wie die Mitgliedstaaten dies bewerkstelligen sollen, bleibt indes völlig offen.[33]

IV. Der Blick nach vorn – Einige Anmerkungen zur Richtlinienumsetzung

Mit Inkrafttreten der Whistleblower-Richtlinie ist auch der deutsche Gesetzgeber zur Umsetzung der Richtlinie in nationales Recht aufgefordert.

1. Bedeutsame Änderungen der gegenwärtigen Rechtslage

Dabei wird sich für das deutsche Recht mit Blick auf die Vorgaben der Richtlinie einiges in puncto Whistleblowerschutz ändern *müssen*. Die rechtlichen Änderungen sind teils einschneidend und ziehen einen vorübergehenden Schlussstrich unter teils langjährige Debatten. Hier allein besonders hervorzuheben ist der eben von Herrn *Franzen* im Detail dargestellte *Kündigungsschutz des extern meldenden Arbeitgebers*:[34] Ungeachtet irgendwelcher Loyalitätsüberlegungen genießt der Hinweisgeber künftig auch dann (Kündigungs-)Schutz, wenn er sich direkt „nach außen" an die zuständige Behörde wendet.[35]

2. Einige Anmerkungen zur Ausgestaltung der nationalen Umsetzungsspielräume

Jenseits der notwendigen Umsetzung zwingender Richtlinienvorgaben in nationales Recht, stellt sich für den deutschen Gesetzgeber die Frage, wie er die vorhandenen Spielräume auf nationaler Ebene nutzt. So könnte er die Richtlinienumsetzung zum Anlass nehmen, den Hinweisgeberschutz auch jenseits des harmonisierten Bereichs der Richtlinie in allgemeiner Weise umfassend zu regeln, wie dies von verschiedener Seite schon seit langem gefordert wird.[36] Er könnte seine Tätigkeit aber auch auf das Nötigste beschränken und es bei einer „1:1"-Umsetzung belassen. Mit wieviel Elan sich der Gesetzgeber der umzusetzenden Rechtsmaterie annimmt, hängt davon ab, für wie überzeugend er die europäischen Regelungen hält. Insofern ist daran zu erinnern, dass der Bundesrat bereits den Richtlinienvorschlag der Kommission heftig kritisiert hatte. Insbesondere die Erstreckung der Richtlinie auf den öffentlichen Sektor war dem Bundesrat ein Dorn im Auge.[37] Zudem war Deutschland neben dem Vereinigten Königreich der einzige Mitgliedstaat, der sich bei der Zustimmungsentscheidung des Rats zur Richtlinie enthalten hatte. Auf der anderen Seite findet sich in Deutschland eine engagierte Lobby für einen starken, weit ausgebauten Hinweisgeberschutz. Angesichts dieser Frontstellung ist im Rahmen der Umsetzungsdebatte eine Fortsetzung des politischen Kampfes zu erwarten.[38] Vor diesem Hintergrund soll im Folgenden zu einigen ausgewählten Aspekte der Richtlinienumsetzung Stellung genommen werden.[39]

2.1 Hinweisgeberschutzgesetz versus Artikelgesetz

Neben zahlreichen materiell-rechtlichen Fragen hat der deutsche Umsetzungsgesetzgeber zunächst die eher „technische", gleichwohl grundlegende Entscheidung zu treffen, ob er die Neuerungen des Hinweisgeberschutzes im Rahmen eines Artikelgesetzes auf die angesprochenen Rechtsgebiete verteilt oder sie in einem neu zu schaffenden Hinweisgeberschutzgesetz zusammenzieht. Zur Vermeidung von Redundanzen, vor allem aber zur Herstellung einer besseren Verständlichkeit für Normadressaten und Rechtsanwender ist ein einheitliches Hinweisgeberschutzgesetz, das die Regelungen im Zusammenhang darstellt und Querbezüge offenlegt, jedenfalls vorzuziehen.[40] So wird auch der Gefahr vorgebeugt, dass im Lichte der Richtlinienvorgaben einheitlich auszulegende Rechtsvorschriften in ihren jeweiligen Regelungszusammenhängen unterschiedlich interpretiert werden. Dies schließt jedoch nicht aus, Sonderfragen für einzelne Rechtsgebiete in den jeweiligen Spezialgesetzen zu regeln. Jedenfalls bedarf es gesetzlicher Verweise aus den Spezialgesetzen auf das zur Anwendung kommende Hinweisgeberschutzgesetz. Das neue Hinweisgeberschutzgesetz hätte dann eine Ordnungs- und Koordinierungsfunktion. Es wäre gleichsam „Schaltstelle" und „Drehscheibe" des neuen Whistleblowing-Regimes in Deutschland.

Ausnahme in Art. 15 Abs. 2 WBRL.

22 Siehe Art. 8 WBRL für weitere Details zum erfassten Personenkreis und möglichen Ausnahmen.

23 Siehe zum Vertraulichkeitsgebot auch noch den für interne wie externe Meldeverfahren geltenden Art. 16 WBRL.

24 Erwägungsgrund 92 WBRL spricht daher von „rechtmäßig" erlangten oder verschafften Dokumenten.

25 Ausführlich hierzu *Johnson*, CCZ 2019, 66 ff.; durchaus kritisch *Garden/ Hiéramente*, BB 2019, 963, 966.

26 Siehe bereits zum Kommissionsvorschlag *Schmolke*, AG 2018, 769, 779.

27 Dazu bereits eingangs sub I.

28 Siehe auch *Gerdemann* (Fn. 4), sub 7.

29 Siehe dazu auch Erwägungsgründe 24 f. WBRL.

30 Siehe zur *Snowden*-Affäre etwa die literarische Aufarbeitung von *Greenwald*, No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State, 2014.

31 Siehe dazu bereits *Schmolke*, ZGR 2019, 909 f. mit Fn. 203.

32 Siehe auch Erwägungsgrund 34 S. 2 WBRL.

33 Erwägungsgrund 47 WBRL trägt zur weiteren Klärung auch nichts Wesentliches bei. Siehe für eine Anregung, wie eine solche „Bestärkung" aussehen könnte, noch unten unter IV.2.6.

34 Siehe zum Folgenden bereits *Schmolke*, ZGR 2019, 876, 894 f. m.N.

35 Siehe oben III.1; zur bereits aktuell bestehenden Überlagerung der Rechtsprechungsgrundsätze durch auf EU-Recht zurückgehendes, sektorspezifisches Sonderarbeitsrecht, siehe näher *Gerdemann*, Transatlantic Whistleblowing, 2018, S. 399 ff sowie 405 ff.; speziell zum Finanzaufsichtsrecht *Helm*, BB 2018, 1538 ff.

36 Siehe zu den bislang erfolglosen Bemühungen um eine nationale Regelung zum Hinweisgeberschutz hier nur die knappe Skizze bei *Schmolke*, AG 2018, 769 m.w.N.

37 Siehe BR-Drs. 173/18 (Beschluss). Siehe dazu näher bereits *Schmolke*, AG 2018, 769, 774 f.

38 Siehe zur Veröffentlichung des Positionspapiers von *Whistleblower Netzwerk e.V.* sowie *Transparency International Deutschland* gleich am Tag der Ratszustimmung siehe bereits eingangs unter I. bei Fn. 3.

39 Siehe zum notwendigen Abgleich mit erst kürzlich erlassenen Gesetzen oder laufenden Gesetzesvorhaben näher *Sonnenberg*, BB 2019, Heft 46, S. I. Dieser Aspekt der Umsetzung wird im Folgenden nicht im Fokus der Betrachtung stehen.

40 Siehe auch *Gerdemann* (Fn. 4), Empfehlung 1 sub 6.

2.2 Anwendungsbereich der neuen Regelungen

Die wohl bedeutendste (rechts-)politische Frage der Umsetzung ist jedoch diejenige nach dem Anwendungsbereich der neuen Regelungen.

2.2.1 Erfasste Rechtsverstöße: Minimalumsetzung oder umfassende Regelung?

Dies betrifft zuvörderst die Frage, ob das neue Whistleblowerschutz-Regime lediglich für die Meldung der in der Richtlinie genannten Verstöße gegen EU-Recht gelten soll oder auch Verstöße gegen andere Rechtsvorschriften, insbesondere auch nationales Recht, erfassen soll. Wie gesehen legt die Richtlinie den Mitgliedstaaten Letzteres nahe. Die Erwägungsgründe halten eine solche Ausweitung des Anwendungsbereichs sogar für erforderlich, „um auf nationaler Ebene für einen umfassenden und kohärenten Rahmen für den Hinweisgeberschutz zu sorgen“.[41] Damit ist das entscheidende Argument gegen eine bloße „1:1“-Umsetzung und für eine ambitionierte Regelung genannt. Selbst wenn man bestimmte Regelungen der Richtlinie nicht für vollständig geglückt hält,[42] erscheint es kaum begründbar, den nationalen Hinweisgeberschutz auf die in der Richtlinie genannten EU-Rechtsverstöße zu beschränken.[43] Vielmehr reicht die soziale Nützlichkeit des Whistleblowing als Rechtsdurchsetzungsinstrument[44] über den Anwendungsbereich der Richtlinie hinaus.

Ist damit im Grundsatz die Schaffung einer umfassenden Hinweisgeberregelung zu befürworten,[45] sollte diese nicht einfach pauschal die Meldung sämtlicher Verstöße gegen nationales Recht einbeziehen.[46] Denn hierbei würde man außer Acht lassen, dass die Förderung des Whistleblowing Kosten verursacht, die mit den Kosten des jeweiligen Rechtsverstoßes abzugleichen sind.[47] Der deutsche Gesetzgeber sollte daher eine bewusste Auswahl der vom Hinweisgeberregime erfassten Rechtsverstöße treffen. Bei der Aufbereitung und Präsentation dieser Auswahl im Rahmen eines neuen Hinweisgeberschutzgesetzes[48] ist freilich auch zu berücksichtigen, dass der Hinweisgeber typischerweise juristischer Laie ist.[49]

2.2.2 Schutz auch bei Meldung bloßen „Fehlverhaltens“?

Das gemeinsame Positionspapier des *Whistleblower Netzwerks* und von *Transparency International Deutschland* spricht sich zudem dafür aus, auch die Meldung „sonstige[n] Fehlverhalten[s], dessen Meldung im allgemeinen öffentlichen Interesse liegt“, in den Anwendungsbereich eines künftigen Hinweisgeberschutzgesetzes aufzunehmen.[50] Eine entsprechende Forderung war bereits auf europäischer Ebene gescheitert,[51] und zwar völlig zu Recht. Eine solche Ausdehnung des spezifischen Hinweisgeberschutzes auf rechtmäßiges (!), aber irgendwie „anstößiges“ oder „unethisches“ Verhalten bärge kaum berechenbare, potenziell schwerwiegende Gefahren, weil es nicht selten an objektiven und rechtssicher handhabbaren Kriterien fehlt, um die Einordnung als „anstößig“ oder „unethisch“ zu treffen. Ebenso lässt sich trefflich darüber streiten, was „im öffentlichen Interesse“ liegt und was diesem zuwiderläuft. Das Whistleblowing drohte daher als politisches oder weltanschauliches Kampfmittel missbraucht zu werden. Dies würde wiederum die gesellschaftliche Akzeptanz dieses für die Rechtsdurchsetzung (!) so wertvollen Instruments gefährden.[52] Kurzum: Von einer Ausweitung des Hinweisgeberschutzes auf (Fehl-)Verhalten, das keinen Rechtsverstoß darstellt, kann nur dringend abgeraten werden.

2.3 Zurückhaltung bei der Ausgestaltung interner Meldeverfahren für den privaten Sektor

Aufgrund der Vorgaben der Richtlinie liegt die Einrichtung eines internen Hinweisgebersystems für die erfassten Unternehmen nicht mehr in deren Organisationsermessen.[53] Zudem setzt die Richtlinie Mindeststandards für die Ausgestaltung eines solchen internen Systems.[54] Jenseits dieser Standards sollte es der Gesetzgeber den Unternehmen jedoch weitgehend selbst überlassen, wie sie ihr Hinweisgebersystem im Einzelnen organisieren. Die Erwägungsgründe der Richtlinie bringen die Vorteile einer solchen Zurückhaltung mit großer Klarheit zum Ausdruck. Dort heißt es: „Welche Personen oder Abteilungen innerhalb einer juristischen Person des privaten Sektors am besten geeignet sind, Meldungen entgegenzunehmen und Folgemaßnahmen zu ergreifen, hängt von der Struktur des Unternehmens ab“.

2.4 Behandlung anonymer Meldungen

Art. 6 Abs. 2 WBRL stellt es den Mitgliedstaaten anheim, ob sie die internen Meldestellen und die für externe Meldungen zuständigen Behörden verpflichten, anonyme Hinweise entgegenzunehmen und weiterzuverfolgen. Diese „weiche“ Regelung will offenbar einer verbreiteten Skepsis gegenüber anonymen Meldungen Rechnung tragen.[55] Indes hängt die Meldebereitschaft potenzieller Hinweisgeber häufig ganz wesentlich davon ab, anonym bleiben zu können.[56] Ein attraktives, praktisch wirksames Hinweisgebersystem kann daher kaum darauf verzichten, auch für anonyme Meldungen offen zu stehen. Vor diesem Hintergrund sollte der deutsche Umsetzungsgesetzgeber die Pflicht interner und externer Stellen zur Entgegennahme und Weiterverfolgung von Hinweisen auch auf anonyme Meldungen erstrecken.[57]

2.5 Voraussetzungen für den Schutz beim Gang an die Öffentlichkeit

Die in Art. 15 Abs. 1 WBRL statuierten Voraussetzungen für den Schutz des Hinweisgebers, der an die Öffentlichkeit geht, sind zu Recht hoch.[58] Die strengen Vorgaben sind hier erforderlich, um den auch grundrechtlich geschützten Interessen der von der Meldung betroffenen Personen in angemessener Weise Rechnung zu tragen.[59] Im Zuge der beginnenden Umsetzungsdiskussion wird nun mit Blick auf eine Verbotsausnahme im GeschGehG für die Offenlegung von Geschäftsgeheimnissen durch Whistleblower die Frage aufgeworfen, ob man von diesen hohen Vorgaben zugunsten des Hinweisgebers abweichen sollte.[60] Angesichts der angesprochenen, durchaus gewichtigen Gegeninteressen der von der Veröffentlichung betroffenen Personen erscheint es jedoch kaum sachgerecht, den laxeren Standard des GeschGehG zum Muster für den allgemeinen Hinweisgeberschutz zu machen.[61] Vielmehr stellt sich umgekehrt die Frage, ob die Vorschrift des GeschGehG nicht möglicherweise einschränkend auszulegen ist, um eine praktische Konkordanz der auf beiden Seiten betroffenen Grundrechtspositionen zu erreichen.

2.6 Ceterum censeo – Finanzielle Anreize für Hinweisgeber

Schließlich bietet die Umsetzung der Whistleblower-Richtlinie dem deutschen Gesetzgeber die Möglichkeit, noch einmal über die Einführung von Belohnungsprogrammen für Hinweisgeber nachzudenken. Solche finanziellen Anreize zur Erhöhung der Meldebereitschaft schaffen auch bei Einführung eines schlagkräftigen Hinweisgeberschutzes einen nicht zu leugnenden Zusatznutzen.[62] Würde man die Auszahlung der Belohnung jedenfalls grundsätzlich an die Einhaltung der Meldefolge intern-extern knüpfen[63], läge darin auch eine wirkungsvolle Maßnahme i.S.d. Art. 7 Abs. 2 WBRL.[64] Der deutsche Gesetzgeber sollte daher noch einmal sorgfältig darüber nachdenken, ob er die Einführung eines kohärenten Hinweisgeberschutzregimes nicht nutzen möchte, um den Einsatz finanzieller Anreize für Whistleblower zu erproben.

V. Zusammenfassung der Ergebnisse

1. Die Verabschiedung der neuen Whistleblower-Richtlinie bietet dem deutschen Umsetzungsgesetzgeber die Gelegenheit, ein kohärentes Hinweisgeberschutzregime in Deutschland einzuführen. Hierfür scheint es schon aus Gründen des besseren Zugangs für potenzielle Whistleblower und (sonstige) Rechtsanwender sinnvoll, die maßgeblichen Bestimmungen im Zusammenhang eines Hinweisgeberschutzgesetzes zu regeln.
2. Die rechtspolitisch wohl bedeutendste Frage der Umsetzung betrifft den sachlichen Anwendungsbereich des neuen Hinweisgeberschutzregimes.
a) Zur Schaffung einer kohärenten Regelung sollte sich die deutsche Umsetzung nicht auf die Meldung der von der Richtlinie erfassten EU-Rechtsverstöße beschränken, sondern den Hinweisgeberschutz auch auf die Meldung weiterer Rechtsverstöße erstrecken. Der deutsche Gesetzgeber sollte hierbei jedoch eine bewusste Auswahl treffen, die für den potenziellen Hinweisgeber verständlich und transparent aufbereitet werden muss.
b) Von der Ausweitung des Hinweisgeberschutzregimes auf die Meldung von bloßem „Fehlverhalten“, das zwar rechtmäßig ist, aber dem öffentlichen Interesse zuwiderlaufen soll, ist mit Nachdruck abzuraten. Es stünde nämlich zu befürchten, dass das Whistleblowing als politisches Kampfmittel eingesetzt wird. Dies aber würde seine gesellschaftliche Akzeptanz als Rechtsdurchsetzungsinstrument gefährden.
3. Jenseits der zwingenden Vorgaben der Richtlinie und der grundrechtlich geforderten Schutzvorkehrungen für die verdächtigten Personen sollte der deutsche Gesetzgeber weitgehend auf konkrete Vorgaben zur Ausgestaltung interner Hinweisgebersysteme durch private Unternehmen verzichten. So erhalten diese die Möglichkeiten, das interne System – im Rahmen der zwingenden Anforderungen – auf die konkrete Realstruktur ihres Unternehmens zuzuschneiden und unnötige Kosten zu vermeiden.
4. Die Meldebereitschaft potenzieller Hinweisgeber hängt häufig ganz wesentlich von der Möglichkeit ab, anonym bleiben zu können. Das neue Hinweisgeberschutzregime sollte daher die Pflicht interner und externer Stellen zur Entgegennahme und Weiterverfolgung von Hinweisen auch auf anonyme Meldungen erstrecken.

41 Siehe dazu bereits o. unter III.2 pr.
42 Siehe zu den (besseren) Argumenten für einen Vorrang interner Meldung *Schmolke*, ZGR 2019, 876, 906 ff.; *ders.*, AG 2018, 769, 777 f.
43 In diesem Sinne auch *Gerdemann* (Fn. 4), sub 1.
44 Siehe dazu ausführlich *Schmolke*, ZGR 2019, 876, 887 ff.
45 So auch *Gerdemann* (Fn. 4), sub 1; *Sonnenberg*, BB 2019, Heft 46, S. I.
46 Vgl. aber *Gerdemann* (Fn. 4), sub 1: „Der Anwendungsbereich der Richtlinie ist bei ihrer Umsetzung umfassend auf nationale Regelungssachverhalte auszudehnen, wozu jedenfalls Straftatbestände und unternehmensrechtliche Bußgeldtatbestände i.S.v. § 30 OWiG zählen.“ In diesem Sinne offenbar auch *Sonnenberg*, BB 2019, Heft 46, S. I.
47 Siehe näher zu diesem Kalkül *Schmolke*, ZGR 2019, 876, 892.
48 Zur vorzugswürdigen Umsetzung der Richtlinie in einem solchen Gesetz soeben unter 2.1.
49 Diesen Aspekt in den Vordergrund stellend *Sonnenberg*, BB 2019, Heft 46, S. I.
50 Siehe *Gerdemann* (Fn. 4), sub 1.
51 Siehe dazu näher *Schmolke*, AG 2018, 769,775 f.; *ders.*, ZGR 2019, 876, 903 f.
52 Siehe zum Ganzen näher bereits *Schmolke*, AG 2018, 769,776; *ders.*, ZGR 2019, 876, 903 f. jew. m.w.N.
53 Siehe zur bisherigen aktienrechtlichen Bewertung oben unter IV.1.
54 Siehe dazu bereits oben unter III.1.
55 Siehe *Council of Europe*, Protection of Whistleblowers, Recommendation CM/Rec(2014)7 and explanatory memorandum, 30.4.2014, online: https://rm.coe.int/16807096c7, S. 14, sub 12.
56 Siehe auch *Gerdemann* (Fn. 4), sub 4: „Vor allem, aber nicht nur bei organisationsinternen Kanälen nutzen Whistleblower anonyme Meldekanäle erfahrungsgemäß häufig als Methode der ersten Kontaktaufnahme.“
57 So auch *Gerdemann* (Fn. 4), sub 4; siehe ferner bereits *Schmolke*, AG 2018, 769, 778 f. (zum Kommissionsvorschlag); *ders.*, ZGR 2019, 876, 909 f. m.w.N.
58 Siehe oben unter III.1. bei Fn. 22.
59 Vgl. dazu auch *Schmolke*, ZGR 2019, 876, 907 f.
60 Siehe *Sonnenberg*, BB 2019, Heft 46, S. I.
61 Dies insinuierend *Sonnenberg*, BB 2019, Heft 46, S. I: „Dass der Gang an die Öffentlichkeit verhältnismäßig sein muss, wird jedenfalls bislang nicht ausdrücklich vorgeschrieben. Unterschiedliche Maßstäbe für die Information der Öffentlichkeit sollten aber möglichst vermieden werden.“
62 Siehe dazu wiederum *Schmolke*, ZGR 2019, 876, 912 f. m.w.N.
63 Siehe bereits *Schmolke*, ZGR 2019, 876, 918 zu den Vorteilen eines solchen Regelungsdesigns.
64 Siehe dazu oben unter III.2.

5. Die hohen Voraussetzungen für den Schutz des Hinweisgebers, der direkt an die Öffentlichkeit geht, tragen den auch grundrechtlich geschützten Interessen der von der Meldung betroffenen Personen angemessen Rechnung. Eine Absenkung der Anforderungen ist daher nicht zu befürworten, sofern überhaupt zulässig.
6. Die Umsetzung der Whistleblower-Richtlinie bietet Anlass, noch einmal sorgfältig über die Einführung finanzieller Anreize für Hinweisgeber nachzudenken. Würde man diese an die Meldefolge intern-extern knüpfen, läge hierin auch ein probates Mittel zur „Hinwirkung" auf eine interne Meldung, wie dies Art. 7 Abs. 2 WBRL fordert.

Marie-Theres Tinnefeld, Kristina Harrer-Kouliev,
Thomas Kastning und Roland Hefendehl

Statements zur Podiumsdiskussion

Prof. Dr. Marie-Theres Tinnefeld,
Hochschule für angewandte Wissenschaften München

Die Bedeutung von Informanten für Presse und Demokratie – Nationale Situation und europarechtliche Vorgaben

Einleitung

Die EU-Whistleblower-Richtlinie (2019/1937) soll den Schutz von Hinweisgebern bzw. Informanten steigern. Sie dient einer Kultur der Freiheit, insbesondere der Freiheit der Meinungsäußerung, der Informationsfreiheit und der Presse. In EG (33) der Richtlinie heißt es daher: „Hinweisgeber sind besonders wichtige Informationsquellen für investigative Journalisten. Ein wirksamer Schutz von Hinweisgebern vor Repressalien erhöht die Rechtssicherheit (potenzieller) Hinweisgeber und erleichtert damit die Weitergabe von Hinweisen auch an die Medien. In dieser Hinsicht trägt der Schutz von Hinweisgebern als journalistische Quellen wesentlich zur Wahrung der Überwachungsfunktion investigativer Journalisten in demokratischen Gesellschaften bei." Der Schutz dieser kommunikativen Freiheiten würde allerdings wenig Ertrag bringen, wenn er nicht zugleich mit dem wohl wichtigsten Menschenrecht in der digitalen Gesellschaft in Bezug gesetzt würde, dem Recht auf Privatheit und Datenschutz. Das Bedeutungspotenzial wird zunächst am Beispiel des Whistleblowers *Edward Snowden* gezeigt, der eine nahezu totale globale Massenüberwachung amerikanischer Geheimdienste und damit eine elementare Verletzung von Privatheit und Datenschutz gegenüber investigativen Journalisten offengelegt hat. Sodann werden die Rechtslage in Deutschland und die Perspektiven für Whistleblower nach der EU-Richtlinie angesprochen.

Whistleblowing: Das Beispiel Edward Snowden

Edward Snowden hat in seinem Buch „Permanent Record"[1] den Versuch unternommen, noch einmal einen Rückblick auf die Zeit zu richten, in der er als **Geheimnisträger** die weltweite digitale Massenüberwachung der Telefon- und Internetverbindungen durch CIA und NSA offen gelegt hat. Der Computerfachmann Snowden war für die Aufgabe angeheuert worden, die abgehörten gespeicherten personenbezogenen Daten zu verschlüsseln. Dabei blieben die ursprünglichen Daten – die „core identity" der Überwachten – in chiffrierter Form erhalten.

In seinem Buch zeichnet Snowden eine Art Selbstporträt. Und es stellt sich für Leser und Leserinnen die Frage: War er Whistleblower, Leaker, Denunziant oder Spion? Der Autor spricht davon, dass er mit der Weitergabe von „top secret" Daten an Journalisten etwas getan habe, was für einen Mann in seiner Position sehr gefährlich sei. Er habe aber beschlossen, die **Wahrheit** zu sagen. Anders formuliert: Er hat die schwerwiegenden Verletzungen des Menschenrechts auf Privatheit und Datenschutz durch die Geheimdienste der USA in der Öffentlichkeit angezeigt, indem er seine Unterlagen investigativen, kundigen Journalisten aushändigte, die sie sodann sichteten und in Zeitschriften wie The Guardian veröffentlichten.

Snowden ist somit kein „Leaker" in dem Sinn, dass er geheimes Material etwa über die Webseite von WikiLeaks ungeprüft und ohne Schutz des Persönlichkeitsrechts betroffener Personen der Öffentlichkeit zugänglich gemacht hätte.[2] Er hat sein brisantes Material Journalisten übergeben, die es vor der Veröffentlichung nach den Regeln **publizistischer Sorgfaltspflichten** nachhaltig bearbeitet haben. Snowden ist auch nicht anonym aufgetreten. Er hat sich aber trotzdem dem Verdacht ausgesetzt, ein Verräter von Staatsgeheimnissen und ein Denunziant zu sein, also Täter eines schweren Verbrechens, das ihn lebenslang in eine Gefängniszelle bringen würde. Dies ist ein Risiko, das ein mutiger Whistblower selbst dann eingeht, wenn er versucht, anonym zu bleiben.

Es ist unbestritten, dass Snowden den Medien zutreffende Informationen, keine Fake News, keine sogenannten „Alternativen Fakten" und keine Falschdarstellungen oder Gerüchte

1 Publikationsdatum: 17. September 2019, Constitution Day in den USA.

2 *Tinnefeld et al.*, Einführung in das Datenschutzrecht, 7. Auflage, 2020, 1. Kap. Rn. 57.

lieferte. Er fällt damit unter den Begriff „Whistleblower“ wie er sich etwa auch in der EU-Wistleblower-Richtlinie (EG 58) findet. Es kann an dieser Stelle offen bleiben, ob er ein Organisationsinsider mit einem privilegierten Informationszugang oder nur einer der Organisation extern Verbundener war.

In der berühmten Schrift zur Beantwortung der Frage: „Was ist Aufklärung?“ findet sich von Immanuel Kant der Aufruf „Sapere aude! Habe den Mut, dich deines eigenen Verstandes zu bedienen!“[3] Kant beschreibt darin, warum es die Aufklärung so schwer hat und gibt dafür als Grund an, dass Menschen sich weigern, mündig zu werden, selbst denken zu wollen, um die Kompetenz der Zustimmung und des Nein-Sagens entwickeln und eigene Verantwortung in Staat und Gesellschaft übernehmen zu können.

Ein Whistleblower wie Snowden hat vom Recht der Meinungs- und Informationsfreiheit Gebrauch gemacht und stichhaltige Unterlagen über einen gravierenden Missbrauch staatlicher Überwachungsrechte im Wege der Presse an die Öffentlichkeit gebracht. Seine Intention war und ist klar. Er hat aus innerer Überzeugung den von Geheimdiensten verursachten Niedergang des „right to privacy“ mit **Zivilcourage** sichtbar gemacht. Denn schließlich läuft jede umfassende und geheime private oder staatliche Observierung von Menschen weltweit auf das **Verbot hinaus, privat zu sein**[4] und damit letztlich auf eine Zerstörung des Grund- und Menschenrechts auf Privatheit und Datenschutz, das zugleich eine unverzichtbare Bedingung für ein demokratisches Miteinander ist.

Vor diesem Hintergrund drängt sich die zugespitzte Frage auf: Sind Bürgerinnen und Bürger noch bei Sinnen, wenn sie sich Politikerinnen und Politikern anvertrauen, die sich nicht darum kümmern, was rechtmäßig ist, was der Realität und Wahrheit entspricht und denjenigen, der sie ausspricht, ins Exil treiben?[5]

Informantenschutz im Kontext deutscher Medien

Das deutsche Grundgesetz schützt grundsätzlich die „institutionelle Eigenständigkeit“ der Presse[6] „von der Beschaffung der Information bis zur Verbreitung der Nachricht und Meinung“.[7] Die Informationsfreiheit gehört zu den grundrechtlich verankerten Rechten, die der autonomen **Recherchefreiheit** des Journalisten dienen. Die grundrechtliche Qualifikation eines Zugriffs „aus allgemein zugänglichen Quellen“[8] hat daher „allein explikative und keine einschränkende Wirkung […]“[9]. Das Redaktionsgeheimnis und das damit korrespondierende Schweigerecht der Journalisten sind ein Indiz dafür, dass diese sich aus anderen Quellen, also auch bei Whistleblowern informieren dürfen.

Es liegt auf der Hand, dass viele Skandale ohne mutige Whistleblower nie aufgedeckt worden wären. Sie sind, wenn sie organisationsintern oder -extern schwerwiegende Missstände nicht klären können, auf Öffentlichkeit, insbesondere auf **investigative Journalisten** angewiesen. Diese müssen die Anforderungen für einen kritischen Qualitätsjournalismus erfüllen, der sich u.a. von der Boulevardpresse oder dem Datenjournalismus (*data-driven-journalism*) unterscheidet.

Die Tätigkeit des investigativen Journalisten steht und fällt mit dem **Quellenschutz.** Dem Journalisten steht zwar ein Schweigerecht zu, das sich auf die Person des Informanten, auf dessen Mitteilungen sowie auf alles selbst recherchierte Material bezieht. Nach der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte[10] darf eine Offenlegung der Quellen nur erzwungen werden, wenn ein überragendes öffentliches Interesse daran besteht. Das Bundesverfassungsgericht hat deutlich darauf hingewiesen, dass Durchsuchungen und Beschlagnahmen in einem Ermittlungsverfahren gegen Presseangehörige verfassungsrechtlich unzulässig sind, wenn sie ausschließlich oder vorwiegend dem Zweck dienen, die Person des Informanten zu ermitteln.[11] Geschützt wird allerdings nicht die Person des Informanten, sondern die Vertraulichkeit der Redaktionsarbeit und das Vertrauensverhältnis zwischen Informant und Medienmitarbeiter.[12] Diesem Ziel dienen im Zivil- und Strafprozess das publizistische Zeugnisverweigerungsrecht sowie ein entsprechendes Beschlagnahmeverbot.

Das **publizistische Zeugnisverweigerungsrecht** schützt den Journalisten grundsätzlich davor, Auskünfte über die Person des Informanten geben zu müssen und damit vor dem in den Prozessordnungen vorgesehenen Zeugniszwang. Wenn der Journalist genötigt werden könnte, den Namen des Informanten oder den Inhalt der ihm anvertrauten Mitteilungen preiszugeben, dann würde mit Sicherheit der für die Medientätigkeit notwendige Informationsfluss versiegen und die Aufklärungsaufgabe der Presse in der Demokratie schwer behindert werden.

Welche Kompetenz hat der europäische Gesetzgeber, um Rechte des Whistleblowers im Kontext journalistischer Tätigkeit zu regeln? Da der Gesetzgeber nach Unionsrecht grundsätzlich keine gesetzliche Allzuständigkeit besitzt,[13] ist zu fragen, ob er gesamteuropäisch für den personenbezogenen Schutz der Daten eines Whistleblowers zuständig ist.

Der europäische Gesetzgeber in Brüssel hat eine Datenschutzgrundordnung (2016/679) geschaffen, die seit dem 25. Mai 2018 ihre volle Wirkung in allen EU-Mitgliedstaaten unmittelbar entfaltet, so auch in Deutschland. Sie markiert einen Fortschritt im europäischen Datenschutzsystem und stellt Presse- und Medienunternehmen weitgehend von datenschutzrechtlichen Vorgaben frei.[14] Die Verordnung[15] gibt den Mitgliedstaaten auf, „durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken […], in Einklang [zu bringen]“. Hinter dieser Privilegierung von Presse und Medien steht die zutreffende Erkenntnis, dass eine kritische, investigative Berichterstattung nur dann möglich ist, wenn Presse und Medien nicht Beschränkungen unterliegen, die mit der Funktion ihrer Tätigkeit unvereinbar wären[16]. So liegt es auf der Hand, dass Presse und Medien online und offline ihre grund- und menschenrechtlich gesicherten Funktionen[17] auch dann wahrnehmen, wenn sie nicht nur ohne die Einwilligung betroffener Personen deren personenbezogene Daten verwenden. An dieser Nahtstelle zeigt sich auch, dass es Sinn macht, wenn Presse und Medien die **Auskunft** über die Identität eines Whistleblowers unter bestimmten Voraussetzungen verweigern dürfen. Für die gegebene Situation ist daher die Einschränkung des datenschutzrechtlichen Transparenzgebots gegenüber betroffenen Personen, also Personen, die durch Hinweise eines Whistleblowers belastet werden, zulässig.

Unter dem Regime der DS-GVO ist es zulässig, dass der deutsche Gesetzgeber Ausnahmen vom Auskunftsrecht der betroffenen Person zugunsten des Whistleblowers vorsieht[18]. Der Gesetzgeber hat das Recht, bereichsspezifische Regelungen zum Schutz des Whistleblowers zu treffen, wenn sie **erforderlich** sind,[19] um das Recht auf freie Meinungsäußerung und Informationsfreiheit (Art. 11 GRCh) zugunsten journalistischer Zwecke mit dem Datenschutz (Art. 7 und Art. 8 GRCh) in Einklang zu bringen (Art. 85 Abs. 2 DS-GVO). In jedem Fall müssen aber Ombudspersonen oder Unternehmen, die Hinweisgebersysteme zur Aufdeckung von Rechtsverstößen betreiben, betroffene Personen darüber informieren, dass gegen sie ein Vorwurf erhoben worden ist, auch wenn sie die Identität des Whistleblowers geheim halten dürfen.[20] Die Frage geeigneter Verfahren zum Schutz der Whistleblower ist Gegenstand einer EU-Richtlinie aus dem Jahre 2019.

EU-Richtlinie zum Schutz der Whistleblower

Die EU-Richtlinie (2019/1937) soll unter dem Dach der Meinungs- und Informationsfreiheit (Art. 11 GRCh) den Whistleblower vor Repressalien schützen. Sie kann daher ein zentraler Baustein zum Schutz der Whistleblower auf Unionsebene werden und eine weitgehende Entkriminalisierung der Hinweisgeber erzielen, die eine wichtige Funktion bei der Aufdeckung schwerwiegender Rechtsverstöße, sei es Korruption, Geldwäsche usw., insbesondere aber auch Verletzungen des Rechts auf Privatheit- und Datenschutz haben. Die Richtlinie muss in nationales Recht umgesetzt werden. Es gilt also, die vorhandenen nationalen Gestaltungspielräume zu nutzen und festzustellen, was europarechtlich zulässig ist und was nicht.

Der grundsätzliche Schutz personenbezogener Daten iSd der DS-GVO wird in EG 58 der Richtlinie ausdrücklich betont. Hinweisgeber sollten nur dann geschützt werden, „wenn sie zum Zeitpunkt der Meldung angesichts der Umstände und der verfügbaren Informationen berechtigten Grund haben, dass die von ihnen geschilderten Sachverhalte der Wahrheit entsprechen.[…].“ Den Hinweisgebern sollen geeignete und sichere Meldekanäle zur Verfügung gestellt werden. Diese Maßnahme bezieht sich auch auf die Presse bzw. digitale Medien. Auf diesem Weg könnten geeignete Hinweiskanäle für investigative Journalisten nach Maßgabe des Unionsrechts, insbesondere der DS-GVO zum Schutz des Whistleblowers, aber auch zum Schutz betroffener Personen, die etwa unzulässigen Verdächtigungen oder Verleumdungen ausgesetzt sein könnten, eingerichtet werden. In diesem Kontext würde der bisher unzureichende Schutz von **Informanten**, die gravierende **Missstände in der Öffentlichkeit transparent** machen, stabilisiert. Das gilt gleicherweise für die Presse bzw. die digitalen Medien, die vom EGMR als „Fundament und Basis jeder demokratischen Gesellschaft“ und als „public watchdog“ bezeichnet werden.[21] Denn Presse- und Medienmacht geraten in eine fast zwiespältige Situation, wenn ihre Informanten ohne erforderlichen Schutz bleiben. Ein solcher unionsweiter Schutz wäre daher ein Fortschritt gegenüber ihrer bisherigen unsicheren Lage.

3 Akademie-Ausgabe, Band VIII, S. 34; s.a. *Horaz*, Epist. I, 2, Vers 40.
4 *Tinnefeld et al.*, Einführung in das Datenschutzrecht, 7. Auflage, 2020, 1. Kap., Rn. 133.
5 Zum Problem *Harry G. Frankfurt*, Über die Wahrheit, aus dem Amerikanischen von *Martin Pfeiffer*, 2007, S. 26.
6 Art. 5 Abs. 1 S. 2 GG.
7 BVerfGE 66, 116, 113.
8 Art. 5 Satz 2 2. Hs. GG.
9 *Kübler*, in: *Simon/Weiss* (Hrsg.), FS *Simitis*, 2000, S. 219 f.

10 EGMR v. 21.01.1999, EuGRZ 1999, 54.
11 BVerfGE 117, 244, 245.
12 Siehe aber auch die Neuregelung in § 5 Abs. 1 Ziff. 2 GeschGehG , in der eine wichtige Ausnahme für Hinweisgeber, die ein Geschäftsgeheimnis zur Aufdeckung einer rechtswidrigen Handlung offenlegen, geschaffen wurde.
13 Zum Grundsatz der begrenzten Einzelermächtigung *Streinz*, in: *ders.* (Hrsg.), EUV/AEUV, 3. Auflage, 2018, Art. 296 AEUV, Rn. 5.

14 Art. 85 DS-GVO.
15 Art. 85 Abs. 1 DS-GVO.
16 Vgl. *Dix*, in: *Simitis/Hornung/Spiecker* (Hrsg.), Datenschutzrecht, 2018, Art. 85 DS-GVO Rn. 1.
17 Art. 5 Abs. 1 S. 2; GG, Art. 10 Abs. 1; EMRK, Art. 11 Abs. 2 GRCh.
18 Öffnungsklausel in Art. 23 Abs. 1 lit. i DS-GVO.
19 *Bäcker*, in: *Kühling/Buchner* (Hrsg.) DS-GVO/BDSG, 2. Auflage, 2018, Art. 15 Rn. 75.
20 *Dix*, in: *Simitis/Hornung/Spieker* (Hrsg.) Datenschutzrecht, 2018, § 33 Rn. 83.

21 Siehe z.B. EGMR, EuGRZ 1995, 16.

Kristina Harrer-Kouliev,
Bundesvereinigung Deutscher Arbeitgeberverbände (BDA), Berlin

Die EU skizziert in der Begründung zur Richtlinie ihre Position zum Hinweisgeberschutz. Danach führt sie in Erwägungsgrund 1 der Richtlinie u. a. aus, dass Personen, die eine Bedrohung oder Beschädigung des öffentlichen Interesses befürchten, diese Befürchtung äußern können müssen, ohne Repressalien zu befürchten. In Deutschland und vor allem im deutschen Arbeitsrecht eine Selbstverständlichkeit.

Es liegt im Interesse der Unternehmen, Fehler frühzeitig aufzudecken und abzustellen. Erfolgt ein begründeter Hinweis durch einen Arbeitnehmer kann der Arbeitgeber schnell und effektiv den Fehler beheben und Maßnahmen ergreifen, um solche Probleme in der Zukunft erst gar nicht entstehen zu lassen. Deshalb bestehen bereits heute in vielen Unternehmen Möglichkeiten zur innerbetrieblichen Meldung von Missständen. Die Entscheidung darüber, welche Maßnahmen erforderlich und geeignet sind um gesetzliche Vorgaben zu erfüllen und Missstände abzustellen, muss bei den zuständigen und haftbaren Entscheidungsträgern im Unternehmen verbleiben.

Die Richtlinie geht über das hinaus, was für einen angemessenen Hinweisgeberschutz erforderlich ist. Eine Anpassung muss daher mit Augenmaß erfolgen.

Arbeitsrechtlich relevant sind in diesem Zusammenhang insbesondere die Hierarchie der Meldekanäle und die in der Richtlinie vorgesehenen Beweislastumkehr.

Die Richtlinie etabliert zwar nicht einen ausdrücklichen Vorrang einer internen Meldung, sie normiert aber in Art. 7 Abs. 2 die Vorgabe, dass sich die Mitgliedstaaten dafür einsetzen, dass die interne Meldung gegenüber der externen Meldung bevorzugt werden soll, wenn intern gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien befürchten muss. Im Bereich des Arbeitsrechts spricht vieles dafür, die von der Rechtsprechung des BAG und der Rechtsprechung des EGMR entwickelten Grundsätze weiterhin anzuwenden. Über die vorrangige interne Meldung kann ein angemessener Ausgleich der Interessen zwischen Arbeitgeber und Arbeitnehmer hergestellt werden. Bestehen interne Meldekanäle, die effektiv und ohne Nachteile für Hinweisgeber eine Beseitigung des Missstandes möglich machen, sollte eine interne Meldung vorrangig bleiben.

In Art. 21 Abs. 5 ist eine Beweislastumkehr in Verfahren vor Gericht oder anderen Behörden vorgesehen. Macht ein Hinweisgeber glaubhaft, dass er eine Benachteiligung infolge seiner Meldung oder Offenlegung erlitten hat, obliegt es der Person, die die Benachteiligung veranlasst hat, nachzuweisen, dass diese Maßnahme auf hinreichend gerechtfertigten Gründen basiert.[22] Das bedeutet eine deutliche Veränderung der bestehenden Beweislast, auch im Arbeitsrecht. Im Arbeitsrecht werden Arbeitnehmer, die in zulässiger Weise ihr Rechte ausüben, vor Repressalien geschützt. Flankiert wird der Schutz durch zahlreiche gesetzliche Regelungen, z.B. aus dem Arbeitsschutzgesetz, aber vor allem durch das Maßregelungsverbot nach § 612a BGB. Die Beweislastregelung kann mit § 612a BGB für das Arbeitsrecht als erfüllt angesehen werden. Ein Neustart ist nicht erforderlich. Ein Sonderschutz für Arbeitnehmer, gegenüber welchen eine Maßnahme seitens des Arbeitgebers ergriffen wurde, wollte der Unionsgesetzgeber nicht schaffen.

22 *Thüsing/Rombey*, NZG 2018, 1001, 1006.

Thomas Kastning,
Whistleblower-Netzwerk e.V., Berlin

Nationale und internationale Affären zeigen aktuell wieder einmal eindrucksvoll die Bedeutung von Whistleblowern. Cum-Ex-Dividendenstripping, Geheim-Vereinbarungen mit Toll Collect, Trumps Telefonate mit Selenskyj: Am Anfang der gesellschaftlichen Skandale stehen Menschen, die eine Situation nicht mehr hinnehmen wollen. Sie sind kurz davor, gegen ihr direktes Umfeld vorzugehen, sie stehen unter enormem Druck, in ihnen toben Loyalitätskonflikte und Angst. Whistleblower-Netzwerk setzt sich seit vielen Jahren für den Schutz dieser Menschen ein. Wir haben daher die im Oktober verabschiedete EU-Richtlinie 2019/1937 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (Whistleblowerschutz-Richtlinie) mit Freude begrüßt. Vor allem die hier verankerte Gleichstellung interner und externer Meldung empfinden wir als einen großen Fortschritt. Nur die Wahl zwischen der organisationsinternen Meldung und der Meldung an die zuständige Behörde gibt Whistleblowern die Möglichkeit, den effektivsten Weg zur Abstellung des Missstandes zu finden.

Wie bei vielen anderen EU-Richtlinien auch bietet die Umsetzung in nationale Rechtsakte Raum für Interpretation und Erweiterung. Insbesondere, da in der Whistleblowerschutz-Richtlinie den Mitgliedstaaten bereits in Erwägungsgrund 5 nahegelegt wird, „den Anwendungsbereich der nationalen Bestimmungen auf andere Bereiche auszudehnen, um auf nationaler Ebene für einen umfassenden und kohärenten Rahmen für den Hinweisgeberschutz zu sorgen."

In der Diskussion des vorangegangenen Vortrags erwähnte Prof. Schmolke, Whistleblower-Netzwerk hätte mit dem ausliegenden Papier „Überlegungen zur nationalen Umsetzung der Whistleblowing-Richtlinie" für die Umsetzungsdebatte bereits die „Messer gewetzt". Dabei empfinden wir die in diesem Papier von *Dr. Simon Gerdemann*, *Prof. Ninon Colneric* und *Annegret Falter* herausgearbeiteten Punkte weniger als scharfe Forderungen, sondern eher als Arbeitsvorschläge für eine sinnvolle und machbare Einbettung des Whistleblower-Schutzes in das deutsche Rechtssystem. Gedacht wurde dabei sowohl an die Whistleblower (wie kann ein Gesetz geschrieben werden, das tatsächlich Rechtssicherheit schafft und das die bekannt gewordenen Whistleblower der letzten Jahre geschützt hätte?) als auch an Behörden und Unternehmen (wie bleiben Bearbeitungsverfahren und Zahl der Meldungen bearbeitbar?).

Entsprechend ist Empfehlung 1 des genannten Papiers zu verstehen: „Der Anwendungsbereich der Richtlinie ist bei ihrer Umsetzung umfassend auf nationale Regelungssachverhalte auszudehnen, wozu jedenfalls Straftatbestände und unternehmensrechtliche Bußgeldtatbestände i. S. v. § 30 OWiG zählen. Im Einklang mit § 5 des Gesetzes zum Schutz von Geschäftsgeheimnissen sind zudem Meldungen über sonstiges Fehlverhalten, die im allgemeinen öffentlichen Interesse liegen, zu schützen." Es geht dem Whistleblower-Netzwerk eben nicht um die heute Nachmittag beschriebene „Missachtung einer roten Ampel", sondern vor allem um Straftatbestände sowie Ordnungswidrigkeiten begangen durch juristische Personen und Personenvereinigungen.

Den Begriff des „sonstigen Fehlverhaltens" bringt das Whistleblower-Netzwerk ein, um das neu zu schaffende Whistleblower-Schutzgesetz mit dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) zu harmonisieren. Das erst im April 2019 erlassene GeschGehG beinhaltet Ausnahmen beim Schutz von Geschäftsgeheimnissen, wenn die Offenlegung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens geeignet ist, das allgemeine öffentliche Interesse zu schützen. Als Beispiel, was das sein könnte, werden Auslandsaktivitäten von Unternehmen genannt, „die in den betreffenden Ländern nicht rechtswidrig sind, aber dennoch von der Allgemeinheit als Fehlverhalten gesehen werden" sowie „die systematische und unredliche Umgehung von Steuertatbeständen."[23]

Nur wenn über die eindeutigen Straftatbestände hinausgegangen wird, besteht die Chance auch diejenigen Fälle abzudecken, bei denen es nicht nur um klar Illegales, sondern auch um Illegitimes geht. Oder anders formuliert: Die Ausdehnung auf „Meldungen über sonstiges Fehlverhalten" ist der Vorschlag, ein Gesetz zu schaffen, das die Whistleblower der Cum-Ex-Deals schützen würde, und das hoffentlich auch das Aufzeigen von Pflegenotständen in deutschen Altenheimen und Krankenhäusern schützen würde.

Soweit rund um die Trilog-Verhandlungen zu hören war, kam der größte Widerstand gegen die Whistleblowing-Richtlinie aus dem deutschen Innenministerium. Hier besteht angeblich die Sorge, ein Whistleblowerschutz für Beamte und Angestellte des öffentlichen Dienstes könnte das Treueverhältnis erodieren und damit die Funktionsfähigkeit des deutschen Staates schwächen. In der Tat schafft die Richtlinie mit ihrer Gleichstellung von interner und externer Meldung Beamten und Angestellten des öffentlichen Dienstes die Möglichkeit, jedenfalls im Bereich des Unionsrechts den vorgeschriebenen Dienstweg zu umgehen und sich mit einem konkreten Verdacht direkt an die zuständige Behörde zu wenden. Kritiker übersehen dabei unter anderem, dass beim begründeten Verdacht auf Korruptionsstraftaten bereits seit zehn Jahren eine ähnliche Regelung existiert und bisher keine negativen Effekte feststellbar sind.

Da kaum zu vermitteln sein wird, warum in deutschen Behörden Whistleblower schlechter geschützt werden sollten als in der Privatwirtschaft, bleibt zu hoffen, dass ein deutsches Gesetz für alle potenziellen Whistleblower die gleichen Standards mit den gleichen Anwendungsbereichen schafft.

Nichtsdestotrotz gelten für den öffentlichen Dienst manche relevante Sonderregeln. So erlaubt die Richtlinie eine Bereichsausnahme für den Schutz von Verschlusssachen. Im Rahmen der Ausübung der Informationsfreiheitsgesetze konnte man in den vergangenen Jahren sehen, wie Geheimhaltungsgrade als behördliches Abwehrschild funktionieren können. Um Ihnen ein Gefühl zu geben, wie umfassend von diesem Mittel Gebrauch gemacht wird: 2015 ging die Bundesregierung davon aus, dass im Bundesinnenministerium jährlich ca. 5.500 Dokumente und andere Informationsträger mit einer der drei höchsten Geheimhaltungsstufen klassifiziert werden. Daten aus anderen Behörden existieren genauso wenig wie ein Überblick über die zahlenmäßige Entwicklung.[24]

Daher muss Teil der Debatte über die nationale Umsetzung der Whistleblowing-Richtlinie der Umgang mit Verschlusssachen werden. Geheimhaltung sollte, wie jede gesellschaftliche Norm, regelmäßig neu ausgehandelt werden. Wenn sie, so wie in diesem Fall, sich aus intrinsischen Gründen externer Kontrolle weitestgehend entzieht, ist dieser Aushandlungsprozess umso wichtiger. Wir alle sollten daher dazu beitragen, dass diese langsam aufflackernde Diskussion so breit wie möglich geführt wird.

23 Vgl. BT-Drs. 19/4724, Erwägungsgründe S. 29.

24 Vgl. BT-Drs. 18/3701.

Prof. Dr. Roland Hefendehl,
Albert-Ludwigs-Universität Freiburg

10 Jahre: Alle lieben Whistleblowing

Ich feiere ein kleines Jubiläum: Seit nunmehr 10 Jahren befasse ich mich wissenschaftlich mit dem Whistleblowing. Und ohne jedes Zögern kann ich die Überschrift meiner insoweit ersten Veröffentlichung in der Festschrift für *Knut Amelung* auch heute wiederholen: Alle lieben Whistleblowing.[25] Der böse Vorwurf einer Denunziation ist längst ebenso vergessen wie die niederschmetternde empirische Analyse von *Backes* und *Lindemann*.[26] Damit dieser Höhenflug ungebremst anhält, kümmert sich auch der Gesetzgeber voller Hingabe um den Schutz des Whistleblowers.[27] Er möge ohne Scheu als wertvolles Mitglied der Compliance-Family alle Missstände ans Tageslicht bringen. Die Veredelung soll nunmehr durch die Umsetzung der EU-Whistleblowing-Richtlinie[28] erfolgen.

Ich spiele mal den Partycrasher: Die von mir vorgeschlagene Differenzierung von systemstabilisierenden und systemdestabilisierenden Whistleblowern[29] ist nahezu unbeachtet geblieben,[30] sie hätte aber den Hype möglicherweise ein wenig relativiert. Denn wir lieben diejenigen Whistleblower wie *Edward Snowden,* die unter Inkaufnahme teilweise hoher persönlicher Risiken gegen das Unrecht bzw. gar die Unrechtssysteme kämpfen.[31] Um diese systemdestabilisierenden Whistleblower geht es aber bei allen gesetzlichen Bemühungen überhaupt nicht. Sie werden vielmehr weltweit mit aller Unnachgiebigkeit verfolgt.[32]

Aber verdient nicht auch die andere Gruppe der Whistleblower zumindest Respekt, wenn sie auf Gesetzesverstöße aufmerksam machen? Aus empirischer Perspektive würde ich antworten: Wenn sie es denn täten! Die Untersuchung von *Backes* und *Lindemann* habe ich bereits erwähnt. Die von *Ralf Kölbel* vorgestellten jüngeren Studien kommen zu keinen besseren Ergebnissen. Daneben verweise ich darauf, dass Compliance und Whistleblowing als kongeniale Partner schlicht der Systemstabilisierung dienen und die Whistleblower somit bereits als Apologeten des Neoliberalismus bezeichnet worden sind.[33] Wenn *Nico Herold* in seiner erkenntnisreichen Arbeit über den Whistleblower[34] einer derartigen Analyse keinen gesonderten Mehrwert beimisst,[35] so möchte ich ihm in diesem Punkt nicht beipflichten. Meinetwegen müssen wir uns mit dem derzeitigen wirtschaftlichen System arrangieren. Aber wir sollten uns über die von mir eingeführte Differenzierung zwischen dem systemstabilisierenden und dem systemdestabilisierenden Whistleblower schon bewusst werden, dass wir schlicht einer Stabilisierung des herrschenden Systems das Wort reden, ohne über das Whistleblowing auch nur einen Gradmesser der Schutzwürdigkeit zu erhalten.

Mir drängt sich die folgende Parallele auf: Die Idee eines europäischen Strafrechts hat mit dem Schutz der finanziellen Interessen der Europäischen Union ihren Ausgangspunkt genommen.[36] Möglicherweise hat auch die EU-Whistleblowing-Richtlinie eine vergleichbare Stoßrichtung. Ich zitiere Erwägungsgrund 2: „Auf Unionsebene sind Meldungen und Offenlegungen durch Hinweisgeber eine Möglichkeit, dem Unionsrecht und der Unionspolitik Geltung zu verschaffen."[37] Die Regelung des sachlichen Anwendungsbereichs bestätigt diesen Verdacht, wenn nach Art. 2 Abs. 1 b) „Verstöße gegen die finanziellen Interessen der Union im Sinne von Artikel 325 AEUV" gemeldet werden sollen.[38]

Hier scheint mir einmal mehr die Europäische Union von oben stabilisiert zu werden, wie ich es bezeichne.[39] Ich habe Zweifel, dass die auszumachende Skepsis der Bürgerinnen und Bürger an der europäischen Idee hierüber zu besänftigen ist.

„Alle lieben Whistleblowing", nun gut, fast alle. Mir ist der Topf der Whistleblower ein wenig zu groß, ich hätte lieber zumindest zwei Töpfe gehabt. Zudem würde ich nach dem Gesagten gerne fragen wollen, wem denn die in diesem Topf gebraute Suppe zugutekommen soll.

25 *Hefendehl,* Alle lieben Whistleblowing, in: *Böse/Sternberg-Lieben* (Hrsg.), Grundlagen des Straf- und Strafverfahrensrechts, Festschrift für Knut Amelung zum 70. Geburtstag, 2009, S. 625 ff.
26 *Backes/Lindemann,* Staatlich organisierte Anonymität als Ermittlungsmethode bei Korruptions- und Wirtschaftsdelikten, 2006; zu dieser Untersuchung *Hefendehl* (Fn. 25), S. 617 (625 ff.).
27 So im Gesetz zum Schutz von Geschäftsgeheimnissen (BGBl. 2019 Teil I Nr. 13 S. 466 ff.), vgl. insbesondere § 5 Nr. 2 GeschGehG.
28 Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, abrufbar unter: https://europa.eu/!vN79jH [letzter Abruf: 5.12.2019].
29 *Hefendehl,* Der ungebremste Höhenflug des Whistleblowers, NK 2015, 359 (362 f.).
30 Vgl. aber nunmehr in diese Richtung *Herold,* Government-Whistleblowing – Enthüllung und Kontrolle von staatlichen Missständen, KJ 2019, 336 (341).
31 *Hefendehl* (Fn. 25), S. 617 ff.; *Hefendehl* (Fn.29), NK 2015, 359 (363 f.).
32 *Hefendehl* (Fn. 29), NK 2015, 359 (370).
33 *Bjørkelo/Madsen,* Whistleblowing and neoliberalism: Political resistance in late capitalist economy, Psychology & Society 5 (2013), S. 28 (33 ff.); *Allen,* Whistleblowing and Crimes Against the Market, Psychology & Society 5 (2013), S. 41 ff.
34 *Herold,* Whistleblower: Entscheidungsfindung, Meldeverhalten und kriminologische Bewertung, 2016.
35 *Herold* (Fn. 34), S. 130.
36 *Hefendehl,* Europäisches Strafrecht: bis wohin und nicht weiter?, ZIS 2006, 229 (230).
37 Erwägungsgrund 2 der Richtlinie (EU) 2019/1937, Amtsblatt der Europäischen Union vom 26.11.2019, L 305/17.
38 Art. 2 Abs. 1 b) der Richtlinie (EU) 2019/1937, Amtsblatt der Europäischen Union vom 26.11.2019, L 305/35.
39 *Hefendehl* (Fn. 36), ZIS 2006, 229 (230).

Vigilanz
Kulturen
SFB 1369