Festschrift

ELISABETH LOVREK

Herausgegeben von

Dr. Andreas Konecny
Univ.-Prof. i.R. in Wien

Dr. Gottfried Musger
Senatspräsident des OGH

Dr. Matthias Neumayr
Vizepräsident des OGH i.R., Univ.-Prof. in Linz

Dr. Martin Spitzer
Univ.-Prof. in Wien

Wien 2024
MANZ'sche Verlags- und Universitätsbuchhandlung

Datenschutzwidrig erlangte Beweismittel

Alexander Wilfinger, Wien

Übersicht:

I. Ausgangspunkt*)

A. Datenschutzrechtlich

Die DSGVO hat im Datenschutzrecht bekanntlich kaum einen Stein auf dem anderen gelassen. Bei der anfänglichen Unsicherheit über Newsletter-Versendungen und Namensschilder an Türklingeln – die freilich erstaunlich weite Kreise bis hin zur Befürchtung einer großangelegten Vertuschungsaktion über die *„multikulturelle Realität"* gezogen hat[1]) – ist es dementsprechend nicht geblieben, vielmehr zeigte sich schnell die wirkliche Tragweite des neuen Regimes. Rund um Komplexe wie die Post-[2]) und PCR-Datenlecks,[3]) *Schrems* vs *Facebook*[4]) oder Lehrer-[5]) und Ärztebewertungsplattformen[6]) stellen sich regelmäßig Fragen etwa nach der Reichweite des Auskunfts-[7]) und Löschungsanspruchs[8]) (Art 15, 17) oder nach dem Zusammenspiel von datenschutzbehördlichem und gerichtlichem Rechtsschutz.[9])

---

*) Der Beitrag ist die erweiterte Fassung eines Berufungsvortrags, den der *Autor* an der Universität Osnabrück gehalten hat.

1) Der Standard, 20. 10. 2018, FPÖ glaubt, Türschilder wegen „Vertuschung" statt DSGVO anonym (https://www.derstandard.at/story/2000089748260/fpoe-glaubt-tuerschilder-wegen-vertuschung-statt-dsgvo-anonym, 22. 5. 2023).

2) OGH 10. 8. 2020, 6 Ob 127/20z; 24. 3. 2023, 6 Ob 19/23x.

3) OGH 24. 3. 2023, 6 Ob 227/22h; 24. 3. 2023, 6 Ob 241/22i; 24. 3. 2023, 6 Ob 242/22i.

4) OGH 23. 6. 2021, 6 Ob 56/21k.

5) OGH 2. 2. 2022, 6 Ob 129/21w; 18. 5. 2022, 6 Ob 67/22d.

6) OGH 29. 8. 2022, 6 Ob 198/21t.

7) OGH 18. 2. 2021, 6 Ob 159/20f; 23. 6. 2021, 6 Ob 56/21k; 17. 2. 2023, 6 Ob 20/23v; 24. 3. 2023, 6 Ob 242/22i; 24. 3. 2023, 6 Ob 19/23x.

8) OGH 20. 12. 2018, 6 Ob 131/18k.

9) OGH 2. 2. 2022, 6 Ob 129/21w.

Gleichzeitig hat der europäische Schwung das allgemeine Privatrecht erfasst und vor allem in der ewigen Diskussion um den Ersatz immaterieller Schäden viel Staub aufgewirbelt.[10]) Dass es auch nach Art 82 keinen Schadenersatz ohne Schaden gibt, stellte der EuGH erst kürzlich in der Rs *Österreichische Post* klar,[11]) nachdem manche nationalen Gerichte zuvor schon den bloßen Verstoß genügen lassen wollten.[12]) Ist die Anwendung des Unionsrechts sogar dem EuGH zu abschreckend und zu effektiv, verdeutlicht das aber eindrucksvoll, wie die DSGVO den Datenschutz aus der Peripherie zur *„vielleicht am schwersten wiegende[n] Landnahme auf dem Gebiet des ‚bürgerlichen' Persönlichkeitsrechts"*[13]) geführt hat.

B. Beweisrechtlich

Beweisrechtlich ist eine derartige Landnahme bislang ausgeblieben, obwohl sich Berührungspunkte auch hier ergeben. Vor allem stellt sich die Frage, wie im Beweisverfahren mit DSGVO-widrig erhobenen Daten umzugehen ist, ob also etwa unzulässige Überwachungsvideos, Dashcam-Aufnahmen, Nutzerdaten-Auswertungen oder Chat-Protokolle berücksichtigt werden dürfen.

Vom zivilrechtlichen Klassiker der immateriellen Schäden gelangt man damit zur nicht weniger ewigen Diskussion um rechtswidrig erlangte Beweismittel, die deshalb so schwierig ist, weil beide denkbaren Grundhaltungen ebenso vernünftig wie unbefriedigend sind: Verwertung trotz materiell rechtswidriger Erlangung sichert die Wahrheitserforschung, belohnt den Rechtsbrecher aber mit dem Prozessgewinn; Verwertungsverbote schützen die rechtstreue Partei, können Gerichte aber zur Fällung materiell falscher Urteile zwingen. Die ZPO zieht sich dabei aus der Affäre und regelt das Problem nicht näher, was sich in der einigermaßen unklaren Linie der Rsp niederschlägt, die zwischen der ohne weiteres möglichen Verwertung und der Notwendigkeit einer Interessenabwägung schwankt.[14]) Die völlig herrschende, besonders von *Kodek* geprägte Lehre hat mit der „Trennungsthese" demgegenüber eine eindeutige Position: Aus der materiellrechtswidrigen Erlangung sollen keine Verwertungsverbote folgen.[15])

Wenn dieses Ergebnis maßgebend mit dem Schutzzweck der verletzten materiellrechtlichen Bestimmungen begründet wird, der nicht in den Prozess reiche,[16]) muss es sich nunmehr freilich auf dem Prüfstand der DSGVO behaupten.

---

10) Eingehend *Spitzer*, Schadenersatz für Datenschutzverletzungen, ÖJZ 2019, 629.
11) EuGH 4. 5. 2023, C-300/21, *Österreichische Post* Rz 28 ff; es gibt allerdings keine Erheblichkeitsschwelle: Rz 43 ff.
12) Etwa BAG NZA 2021, 1713 Rz 33; näher *Burtscher*, DSGVO und immaterielle Schäden: erste internationale Entwicklungen, ZEuP 2021, 698.
13) *Rixecker* in MünchKommBGB[9] Anh zu § 12 Rz 12.
14) Überblick bei *Spitzer* in *Spitzer/Wilfinger*, Beweisrecht Vor §§ 266 ff ZPO Rz 31.
15) Siehe nur *Kodek*, Rechtswidrig erlangte Beweismittel im Zivilprozeß (1987) 136 ff; *Kodek*, Die Verwertung rechtswidriger Tonbandaufnahmen und Abhörergebnisse im Zivilverfahren, ÖJZ 2001, 281, 334; *Kodek*, Even if you steal it, it would be admissible – Rechtswidrig erlangte Beweismittel im Zivilprozess, in FS Kaissis (2012) 523; außerdem etwa *Rechberger* in *Fasching/Konecny*[3] Vor § 266 ZPO Rz 70; *Rechberger/Klicka* in *Rechberger/Klicka*, ZPO[5] Vor § 266 Rz 24; diff *Fasching*, Lehrbuch des österreichischen Zivilprozessrechts[2] (1990) Rz 934 ff; krit *Rebhahn*, Geheimnisschutz – Datenschutz – Informationsschutz: System und Prinzipien, in *WiR*, Geheimnisschutz – Datenschutz – Informationsschutz (2007) 1 (30 mit FN 130); *Rebhahn*, Mitarbeiterkontrolle am Arbeitsplatz (2009) 28 f; *L. Schmid*, Anm zu 2 Ob 162/16m, ÖJZ 2018, 75.
16) *Kodek*, ÖJZ 2001, 281 (291 ff); *Kodek* in FS Kaissis 523 (540 ff).

Wie in Deutschland, wo das BVerfG bereits vor mehreren Jahren eine strengere Handhabung zum Schutz des allgemeinen Rechts auf freie Entfaltung der Persönlichkeit (Art 2 Abs 1 GG) einforderte und so zum Taktgeber zivilprozessualer Beweisverwertungsverbote wurde,[17]) könnte das besonders gestärkte Recht auf Datenschutz nämlich auch in Österreich neue Impulse setzen. Lässt sich also der Status quo aufrechterhalten oder gibt es eine europäische Neuauflage des nationalen Klassikers?

II. DSGVO im Beweisverfahren

A. Prozessausnahmen

So naheliegend die Frage zunächst ist, so schnell wird sie regelmäßig wieder verworfen. In einem vor dem Hintergrund der zivilrechtlichen Paralleldiskussion auffallend unbeeindruckten Zugang spricht sich die ganz herrschende Ansicht gegen prozessuale Einflüsse der DSGVO aus, denn diese wolle das Beweisverfahren gar nicht regeln.[18])

Gestützt wird der Befund auf verschiedene Bestimmungen, die die Datenverarbeitung in Gerichtsverfahren besonders behandeln oder sogar explizit erlauben: *Werderitsch* weist auf ErwGr 20 hin, wonach die DSGVO zwar auch für die Tätigkeiten der Gerichte gilt, die dabei notwendigen Datenverarbeitungsvorgänge aber speziell zu regeln sind; § 83 GOG nimmt diesen Auftrag im Sinne einer umfassenden Erlaubnis der Verarbeitung erforderlicher Daten wahr.[19]) Ähnlich aufgeschlossen ist Art 9 über sensible Daten etwa zur ethnischen Herkunft, Weltanschauung, Gesundheit oder sexuellen Orientierung, die zwar nur in wenigen Ausnahmefällen verarbeitet werden dürfen; als solchen erkennt Abs 2 lit f aber die Erforderlichkeit „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit" an,[20]) wobei mit *Rechberger/Klicka* ein Größenschluss hinsichtlich sonstiger, weniger sensibler Daten naheliegt.[21]) Dass zur Sicherstellung der „Durchsetzung zivilrechtlicher Ansprüche" Ausnahmen von den Betroffenenrechten vorgesehen werden dürfen (Art 23 Abs 1 lit j),[22]) der Betroffene einer Verarbeitung zur „Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" nicht wider-

17) BVerfG NJW 2002, 3619; NJW 2003, 2375; BGH JZ 2003, 1109 (krit *Foerste*); näher etwa *Thole* in *Stein/Jonas*, ZPO[23] § 286 Rz 46 ff.

18) *Rechberger/Klicka* in *Rechberger/Klicka*, ZPO[5] Vor § 266 Rz 24; *Klicka*, Beweis(verwertungs)verbote im Arbeitsrecht? ZAS 2020, 20 (23); *Werderitsch*, DSGVO: Beweisverwertungsverbot auf Umwegen? RdW 2021, 242 (243 f); *Werderitsch*, Anm zu 7 Ob 121/22b, EF-Z 2022, 286; *Kodek*, Anm zu 7 Ob 121/22b, ecolex 2022, 977 (978). Anders *Zwettler*, Rechtliche Konsequenzen der Verwendung rechtswidrig erlangter Beweismittel? ecolex 2019, 8 (9 f): eine Interessenabwägung führe regelmäßig zur Zulässigkeit; *Stella/Winter*, AN-Datenschutz: DSGVO, Strafen und Rechtsweg – zentrale Problemfelder, ZAS 2020, 252 (256): Verwertungsverbote kraft DSGVO möglich.

19) *Werderitsch*, EF-Z 2022, 286 (286); s auch *Kodek*, ecolex 2022, 977 (978).

20) Anwendungsbeispiele liefern OGH 24. 7. 2019, 6 Ob 45/19i (Akteneinsicht); LAG Berlin-Brandenburg MMR 2022, 319; LAG Hannover MMR 2023, 313.

21) *Rechberger/Klicka* in *Rechberger/Klicka*, ZPO[5] Vor § 266 Rz 24.

22) *Werderitsch*, RdW 2021, 242 (243); *Ahrens*, Dashcam-Aufzeichnungen als Beweismittel nach Verkehrsunfällen, NJW 2018, 2837 (2839), freilich ohne Rückschluss auf Verwertungsverbote.

sprechen kann (Art 21 Abs 1)[23]) und der Löschungsanspruch bei Erforderlichkeit der Daten zu diesen Zwecken überhaupt sistiert wird (Art 17 Abs 3 lit e),[24]) vervollständigt das Bild.[25])

Insgesamt zeigt sich das Datenschutzrecht also nicht blind gegenüber dem Justizgewährungsanspruch (Art 6 EMRK; Art 47 GRC). Es trägt dem Interesse an Rechtsdurchsetzung vielmehr ebenso Rechnung, wie etwa § 38 Abs 2 Z 7 BWG das Bankgeheimnis zur Klärung von Rechtsangelegenheiten zwischen Bank und Kunden durchbricht.[26]) Neben dem Parteiverhalten billigt es damit auch die Tätigkeit des Gerichts selbst, das ja nicht erst seit dem aktuellen Digitalisierungsschub vom elektronischen Akt bis zur Videoverhandlung ständig mit Daten hantiert.[27]) Der Zivilprozess muss sich eben nicht per se dafür rechtfertigen, zwangsläufig auch ein großer Datenverarbeitungsprozess zu sein.

B. Regelungsanspruch und Vorgaben

1. *Norra Stockholm Bygg:* Urkundenvorlage

Darin liegt aber selbst dann kein beweisrechtlicher Freibrief, wenn man rechtswidrig erlangte Daten vorerst ausklammert und sich zunächst auf unverdächtige Normalfälle der Beweisaufnahme konzentriert. Jüngst hat der EuGH der DSGVO in der schwedischen Rs *Norra Stockholm Bygg*[28]) nämlich auch hierfür durchaus konkrete Vorstellungen entnommen.

Im Ausgangsfall wendete der Beklagte gegen den geltend gemachten Werklohnanspruch ein, die abgerechneten Personalstunden seien überhöht. Zum Beweis beantragte er die Vorlage eines aus steuerlichen Gründen zu führenden Personalverzeichnisses durch einen Dritten, der es im Auftrag des Klägers erstellt hatte. Aus Sorge um die personenbezogenen Daten der darin erfassten Arbeiter sprach sich der Kläger dagegen aus,[29]) womit er zunächst keinen Erfolg hatte: Nachvollziehbarerweise verneinten die Instanzgerichte ein berücksichtigungswürdiges Interesse am Unterbleiben der Offenlegung, sie gaben dem Beweisantrag entsprechend der nach schwedischem Recht grundsätzlich bestehenden Vorlagepflicht statt.[30]) Das Höchstgericht fragte sich allerdings, ob es bei dieser Entscheidung nach rein nationalen Maßstäben bleiben dürfe oder ob der DSGVO

23) Vgl *Klicka*, ZAS 2020, 20 (23).
24) Vgl *Waldkirch*, Die Verarbeitung von Gesundheitsdaten durch Versicherer, VersR 2020, 1141 (1154), der daraus aber zu Recht keine absoluten Schlüsse zieht.
25) Außerdem sichert Art 55 Abs 3, wonach Aufsichtsbehörden nicht für die Aufsicht über Verarbeitungen im Rahmen justizieller Tätigkeit zuständig sind, die richterliche Unabhängigkeit ab; dazu EuGH 24. 3. 2022, C-245/20, *Autoriteit Persoonsgegevens:* Akteneinsicht durch Journalisten.
26) Näher *Spitzer* in *Bollenberger/Oppitz*, Bankvertragsrecht I[3] (2019) Rz 2/145 f sowie 2/176 zur Durchbrechung gegenüber Dritten im Wege einer Interessenabwägung; dazu eingehend *Liebel*, Das zivilrechtliche Bankgeheimnis (2019) 180 ff.
27) *Werderitsch*, RdW 2018, 242 (243 f): Sicherstellung der Funktionsfähigkeit der Justiz.
28) EuGH 2. 3. 2023, C-268/21, *Norra Stockholm Bygg.*
29) Rz 13, 15 ff. Ganz ähnlich LAG Berlin-Brandenburg NZA-RR 2023, 183: Aus Rücksichtnahme auf Daten Dritter verweigerte der beklagte Handelsvertreter Auskunft über unerlaubte Konkurrenztätigkeit.
30) Zum Rechtsrahmen Rz 10 ff, 22 f. Dabei wird offenbar nicht zwischen der Vorlage durch den Gegner oder einen Dritten unterschieden (anders §§ 303 ff, 308 ZPO).

„auch Anforderungen an das nationale Verfahrensrecht in Bezug auf die Vorlegungspflicht zu entnehmen" sind.[31])

Diesen Ball nahm der EuGH gerne auf: Auch die Vorlage eines Dokuments im Zivilprozess fällt in den Anwendungsbereich der DSGVO, sodass die Verarbeitung der darin enthaltenen personenbezogenen Daten den Rechtmäßigkeitsanforderungen des Art 6 entsprechen muss.[32]) Konkret führte die Erkenntnis in die Prüfung einer nur unter besonderen Voraussetzungen zulässigen „Zweckänderung" (Art 6 Abs 4),[33]) weil das Personalverzeichnis ursprünglich nicht mit Blick auf vertragliche Streitigkeiten, sondern in Erfüllung einer verwaltungsrechtlichen Pflicht zur Ermöglichung von Steuerprüfungen erstellt wurde. Eine derartige Änderung könne aufgrund der Notwendigkeit des Beweismittels zur Anspruchsdurchsetzung allerdings gerechtfertigt sein,[34]) was bei der Vorlage von Dokumenten mit personenbezogenen Daten insgesamt beachtlich sei, weil sich Datenschutz mit dem Justizgewährungsanspruch (Art 47 GRC) vereinbaren lassen müsse und allenfalls dahinter zurücktrete.[35]) Stets sei die Verarbeitung personenbezogener Daten aber auf das notwendige Maß zu beschränken („Datenminimierung", Art 5 Abs 1 lit c), weshalb im Einzelfall die Vernehmung ausgewählter Zeugen vorrangig sein könne[36]) oder das Gericht zusätzliche Datenschutzmaßnahmen (Pseudonymisierung, Anonymisierung) ergreifen müsse (Art 4 Nr 5, ErwGr 26).[37])

2. Folgerungen

Was daraus konkret für den österreichischen Urkundenbeweis folgt, ist im gegebenen Zusammenhang nebensächlich. Die Vorgaben werden sich verhältnismäßig leicht in das Vorlagesystem der §§ 303 ff ZPO einfügen lassen, das Beweis- und Geheimhaltungsinteressen sorgsam abwägt;[38]) ein gesetzlicher Anhaltspunkt für nötige Pseudo- oder Anonymisierungen findet sich in § 298 Abs 2 ZPO über die Beschränkung der Einsicht des Gegners auf bestimmte Teile der Urkunde.[39])

Wesentlich ist aber die grundlegende Erkenntnis, dass der Regelungsanspruch der DSGVO den Zivilprozess im Allgemeinen und das Beweisverfahren im Besonderen sehr wohl erfasst. Entgegen dem durch die zahlreichen Prozessausnahmen vermittelten Eindruck[40]) existiert außerdem kein allgemeiner Erlaubnissatz für Zivilverfahren, vielmehr ist die Verarbeitung der konkreten Daten in der konkreten Situation zu beurteilen.[41]) Dabei anerkennt der EuGH zwar den

---

31) Rz 24.
32) Rz 26 ff.
33) Krit *Cepic*, Anm zu EuGH C-268/21, ecolex 2023, 458 (458).
34) Rz 37 ff. Für den Auskunftsanspruch gegen den Handelsvertreter rekurriert das LAG Berlin-Brandenburg NZA-RR 2023, 183 Rz 110 ff überzeugend auf Art 6 Abs 1 lit c (Verarbeitung zur Erfüllung rechtlicher Verpflichtungen), was sich auf die Werklohnklage übertragen lässt.
35) Rz 43 ff, 53.
36) Rz 55.
37) Rz 56 ff; auf die damit verbundenen Schwierigkeiten weist *Cepic*, ecolex 2023, 458 (458 f) hin.
38) Vgl *Wilfinger* in *Spitzer/Wilfinger*, Beweisrecht § 303 ZPO Rz 3 ff.
39) Vgl *Wilfinger* in *Spitzer/Wilfinger*, Beweisrecht § 298 ZPO Rz 4 f.
40) Siehe oben II.A.
41) Vgl zum Verwaltungsrecht auch EuGH 4. 5. 2023, C-60/22, *Bundesrepublik Deutschland* Rz 71 ff.

hohen Stellenwert des Beweisinteresses, das die in der prozessualen Verwendung liegende Datenverarbeitung regelmäßig rechtfertigen wird. Er verhilft ihm aber offenbar nicht um jeden Preis zum Durchbruch, weil nationale Gerichte die Angemessenheit, Erheblichkeit und Verhältnismäßigkeit der Offenlegung personenbezogener Daten prüfen und mögliche Alternativen in Betracht ziehen müssen.[42])

C. Konsequenzen bei rechtswidriger Erlangung

Wirkt sich die DSGVO insofern schon auf die „gewöhnliche" Beweisaufnahme aus, liegen Vorgaben für die gesteigert problematischen Fälle rechtswidrig erlangter Daten umso näher. Wer etwa strenge Anforderungen an die Verarbeitung zu einem anderen Zweck als dem der ursprünglichen Erhebung stellt (Art 6 Abs 4) – aus der Dokumentation für Steuerprüfungen wird ein Beweismittel im Werklohnprozess –, muss die Schrauben bei Verarbeitung ohne rechtmäßige Erhebung – man hätte von vornherein nicht dokumentieren dürfen – ja konsequenterweise noch einmal anziehen.

Das heißt nicht, dass DSGVO-Verstöße zwangsläufig zu Beweisverboten führen müssen.[43]) Die europäische Entwicklung hat den österreichischen Status quo aber überholt. Datenschutz findet gleichermaßen außer- und innerprozessual statt und betrifft die herrschende Trennungsthese damit in ihrem Kern, sodass die kategorische Ablehnung von Verwertungsverboten nicht mehr ohne weiteres überzeugt. Immerhin fordert die DSGVO eine wirksame und abschreckende Sanktionierung von Verstößen (Art 84),[44]) auf nationale Systematik – etwa die oft ins Treffen geführte Unbekämpfbarkeit eines „Zuviels" an Beweisen (§ 496 Abs 1 Z 2 ZPO)[45]) – nimmt sie natürlich keine Rücksicht. Dabei hat der EuGH erfahrungsgemäß keinerlei Berührungsängste gegenüber dem Verfahrensrecht. Neben *Norra Stockholm Bygg* führt das vor allem die Rsp zur Klauselrichtlinie vor Augen, die ein regelrechtes „Klauselprozessrecht" von der Stoffsammlung über die Kostentragung bis zur Rechtskraft entstehen lässt.[46]) In benachbarten Verfahrensordnungen lagen auch Beweisverbote schon auf dem Tisch: Stützt sich ein Abgabenbescheid auf rechtswidrige Überwachungsergebnisse aus einem parallelen Strafverfahren, sind zur Wahrung des Rechts auf Privat- und Familienleben (Art 7 GRC) *„die verwendeten Beweise zurückzuweisen und ist der angefochtene Bescheid, der sich auf diese Beweise gründet, aufzuheben, wenn er deswegen keine Grundlage hat"*.[47])

---

42) Siehe insb EuGH 2. 3. 2023, C-268/21, *Norra Stockholm Bygg* Rz 55.

43) Das betonen auch *Stella/Winter*, ZAS 2020, 252 (256).

44) Vgl *Schild* in BeckOK DatenSR[42] Syst E Rz 39; zum alten Recht *Rebhahn*, Mitarbeiterkontrolle 29.

45) Etwa *Kodek*, ÖJZ 2001, 334 (344); krit jüngst *Rassi*, Kann ein „Zuviel" auch einen Verfahrensmangel begründen? in FS Konecny (2022) 429, wonach der Aspekt der Verwertung rechtswidrig erlangter Beweismittel allerdings der *„(eher) unproblematische Teil der Zuviel-Regel"* sei (434 f). Zu den Möglichkeiten einer Anrufung des OGH *Werderitsch*, EF-Z 2022, 286 (286); *Kodek*, ecolex 2022, 977 (977).

46) Siehe etwa *Geroldinger*, Rechtsdurchsetzung im Verbraucherrecht – prozessuale Aspekte, 21. ÖJT II/1 (2022) 179 ff; *Korp*, Neue Regeln im Zusammenspiel zwischen der Klausel-RL und dem nationalen Verfahrensrecht, ÖBA 2022, 902; *H. Roth*, Kompetenzwidrige Eingriffe des EuGH in die nationalen Zivilprozessrechte, JZ 2023, 100; *Lutschounig*, Klauselprüfung im Mahn- und Vollstreckungsverfahren, ZFR 2023, 108.

47) EuGH 17. 12. 2015, C-419/14, *WebMindLicenses* Rz 89; darauf hinweisend *Thiele/Wagner*, DSG[2] § 12 Rz 99.

Nationale Gerichte haben dieser neuen Facette im Zweifel durch entsprechende Vorlagen Rechnung zu tragen.[48]) Freilich zeigt gerade die verbraucherrechtliche Judikatur der letzten Jahre auch, dass eine engmaschige Befassung des EuGH das Potenzial systemsprengender Überraschungen birgt. Dieser Eindruck muss nicht gleich zu einer Abschottung führen, wie sie namentlich dem BGH vorgeworfen wird, der mitunter eine *„irritierende Verweigerungshaltung"* an den Tag lege.[49]) Sie ermuntert aber zur ernsthaften Prüfung eines *acte clair*, weil auch unter dem neuen Regime nicht alle noch unentschiedenen Fragen tatsächlich zweifelhaft sind. Sichtet man das bisherige Fallmaterial,[50]) lässt sich jedenfalls einiges abschichten.

III. Fallgruppen

A. Rechtmäßige Erlangung

Das führt zunächst zur bisher einzigen einschlägigen Entscheidung des OGH.[51]) Die Antragstellerin beantragte die Erlassung einer einstweiligen Verfügung, weil der Gegner sie mit einer Spitzhacke attackiert habe, was durch ein Handyvideo dokumentiert sei. Wer hinsichtlich der Erfolgschancen des Antrags auf dieser Grundlage optimistisch ist, hat die Rechnung ohne das Erstgericht gemacht, das den Antrag umgehend abwies, *„weil der Antragsgegner als gefilmte Person in die Verarbeitung der personenbezogenen Daten nicht aktiv eingewilligt habe".* Das Rekursgericht korrigierte die Entscheidung und wurde vom OGH bestätigt. Aus der DSGVO folge nämlich *„kein generelles Beweisverwertungsverbot"* für datenschutzwidrig erlangte Beweismittel, die Notwendigkeit einer Interessenabwägung auf beweisrechtlicher Ebene könne angesichts der klaren Ausgangslage dahinstehen.

Dieses Ergebnis überzeugt ohne weiteres, die Einleitung eines Vorabentscheidungsverfahrens wurde zu Recht nicht erwogen. Auf den zweiten Blick drängt sich aber die Frage auf, ob die Diskussion um rechtswidrig erlangte Beweismittel dafür überhaupt bemüht werden musste.[52]) Die erstgerichtlichen Bedenken zur fehlenden Zustimmung des Gefilmten lassen sich ja bereits einen Schritt früher verwerfen: In der konkreten Situation eines Spitzhacken-Angriffs wird die Aufnahme schon gar nicht rechtswidrig gewesen sein, weil die vorgelagerte datenschutzrechtliche Interessenabwägung (Art 6 Abs 1 lit f; § 12 Abs 2 Z 4 DSG)[53]) zweifellos zugunsten der Angegriffenen ausgeht.[54])

Bei aller Unklarheit über mögliche Rechtsfolgen sollte die wesentliche Vorfrage des DSGVO-Verstoßes also nicht aus den Augen verloren werden. Erlaubt das Datenschutzrecht die Datenerhebung von vornherein, stellt sich das Problem rechtswidrig erlangter Daten natürlich nicht, die prozessuale Verwendung richtet sich dann vielmehr nach den – wie *Norra Stockholm Bygg* zeigt: ebenfalls DSGVO-

48) *Spitzer* in *Spitzer/Wilfinger*, Beweisrecht Vor §§ 266 ff ZPO Rz 33.
49) *Graf von Westphalen*, Irritierende Verweigerungshaltung des BGH (Art 267 Abs 3 AEUV), ZIP 2022, 1465.
50) Umfassende Darstellungen etwa bei *Prütting* in MünchKommZPO[6] § 284 Rz 68 ff; *Thole* in *Stein/Jonas*, ZPO[23] § 286 Rz 57 ff.
51) OGH 24. 8. 2022, 7 Ob 121/22b EF-Z 2022, 285 *(Werderitsch)* = ecolex 2022, 976 *(Kodek)* = EvBl 2023, 241 *(Wilfinger)*.
52) Siehe schon *Wilfinger*, Anm zu 7 Ob 121/22b, ÖJZ 2023, 243 (243 f).
53) Näher *Thiele/Wagner*, DSG[2] § 12 Rz 72 ff.
54) Siehe auch *Werderitsch*, EF-Z 2022, 286 (287); *Kodek*, ecolex 2022, 977 (977).

determinierten – allgemeinen Regeln der Beweisaufnahme und -verwertung.[55]) Im Einzelnen ist diese Selbstverständlichkeit freilich weniger trivial, weil die inhaltlich maßgebenden Überlegungen ineinandergreifen.[56]) Dabei führt die regelmäßig ausschlaggebende Frage, inwieweit Beweiszwecke die Datenerhebung rechtfertigen, mitunter in datenschutzrechtliche Untiefen. In einem familiären Streit gelangte der OGH etwa erst nach einer aufwendigen datenschutz- und persönlichkeitsrechtlichen Prüfung zum Ergebnis, dass das anlassbezogene Filmen von verbalen Ausfälligkeiten und körperlichen Übergriffen vor einem Vereinslokal zulässig war.[57]) Vor dem deutschen BAG konnte ein Arbeitgeber die Rechtmäßigkeit der ausgesprochenen Kündigung beweisen, weil eine erlaubte offene Videoüberwachung der betroffenen Trafik zeigte, dass die gekündigte Verkäuferin in die Kasse gegriffen hatte.[58]) Genauso lässt sich verbotene private Internetnutzung am Arbeitsplatz mit einer entsprechenden Datenauswertung belegen, wenn es hierfür eine datenschutzrechtliche Grundlage gibt, wie sie das LAG Köln in § 26 Abs 1 BDSG fand.[59]) In einer rezenten Entscheidung zur elektronischen Akte des deutschen Bundesamts für Migration und Flüchtlinge, die Verwaltungsgerichten im Rahmen eines gemeinsamen Verfahrens (Art 26) übermittelt wird, verneinte schließlich auch der EuGH Konsequenzen für das verwaltungsgerichtliche Verfahren; die fraglichen „technischen" Verstöße gegen Art 26 (fehlende Vereinbarung der Verantwortlichen) und Art 30 (fehlendes Verzeichnis der Verarbeitungstätigkeiten) stellten gegenüber dem Betroffenen nämlich gar *„keine unrechtmäßige Verarbeitung"* dar.[60])

Die Beurteilung verlagert sich in solchen Fällen vollständig auf die Ebene des Datenschutzrechts und wird dadurch nicht zwingend leichter. Immerhin umschifft man aber die prozessualen Untiefen, weil sich mit der Rechtswidrigkeit auch die rechtswidrig erlangten Beweismittel erübrigen.

B. Beweisrechtlich unbeachtliche Verstöße

1. Dashcam

Selbst bei feststehender rechtswidriger Erlangung hält sich das Bedürfnis nach Verwertungsverboten indes häufig in Grenzen. Das veranschaulicht die bekannte Dashcam-Entscheidung des BGH:[61]) In einem Verkehrsunfallprozess bot der klagende Geschädigte zum Beweis des Unfallhergangs ein Video an, das eine im Frontbereich seines Kfz installierte Kamera aufgenommen hatte. Datenschutzrechtlich ist die Zulässigkeit solcher Dashcams ein *„äußerst heikle[r] Themen-*

55) Dazu oben II.B.
56) Eingehend *Niemann*, Keylogger & Co: Verwertungsverbote infolge grundrechtswidriger Arbeitgebermaßnahmen, Jahrbuch des Arbeitsrechts 55 (2018) 41 (45 ff).
57) OGH 20. 5. 2020, 6 Ob 206/19s.
58) BAG NZA 2018, 1329.
59) LAG Köln ZD 2020, 533; näher zu dieser Grundlage *Thüsing/Rombey*, Der verdeckte Einsatz von Privatdetektiven zur Kontrolle von Beschäftigten nach dem neuen Datenschutzrecht, NZA 2018, 1105; s auch *Niemann*, Jb Arbeitsrecht 55 (2018) 41 (57).
60) EuGH 4. 5. 2023, C-60/22, *Bundesrepublik Deutschland* Rz 74; zur Argumentation mit Art 6 Art 1 lit e (Rz 73) noch unten III.C.
61) BGH NJW 2018, 2883 = JZ 2018, 935 (krit *Heese*); dazu etwa *Ahrens*, NJW 2018, 2837; *Schweiger/Werderitsch*, Verwertung von Dashcam-Aufnahmen im Zivilprozess, Zak 2018, 187; zuvor schon *Thole*, Beweisverwertungsverbot für Dashcam-Aufzeichnungen im Verkehrsunfallprozess? in FS Prütting (2018) 573.

komplex", weil anlassloses Filmen des Verkehrsgeschehens als Beweissicherung für mögliche Unfälle zwar nachvollziehbar ist, aber massenhaft in das Persönlichkeitsrecht unbeteiligter Dritter eingreift.[62]) Im Wesentlichen werden daher Einschränkungen mit Blick auf Bildqualität und Speicherdauer diskutiert; der BGH ging davon aus, dass *„im Sinne eines zumutbaren mildesten Mittels […] lediglich eine kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen"* erlaubt sei. Diesen Anforderungen wurde die breitflächig aufzeichnende Kamera des Klägers aber nicht gerecht,[63]) sodass es sich beim Unfallvideo tatsächlich um ein datenschutzwidrig erlangtes Beweismittel handelte.

Dennoch bejahte der BGH die Verwertbarkeit nach Vornahme einer Interessenabwägung. Das Beweisinteresse des Klägers rechtfertige den Eingriff in das Persönlichkeitsrecht des gefilmten Unfallgegners, der sich ja freiwillig in der Öffentlichkeit bewegt habe und deshalb nur geringfügig in seiner Sozialsphäre betroffen sei.[64])

Ausgehend vom Schutzzweck des Dashcam-Verbots ist diese Lösung konsequent. Liegt der Grund für die Datenschutzwidrigkeit in der überschießenden Aufnahme beliebiger Verkehrsteilnehmer, wirkt sie sich gegenüber dem konkreten Unfallgegner ja nicht aus. Der Gegner darf gefilmt werden, eine *„kurzzeitige anlassbezogene Speicherung im Zusammenhang mit einem Unfallgeschehen"* wäre erlaubt gewesen. Warum sollte man ihm das Video dann nicht vorhalten dürfen? Das unterstreichen zwei Kontrollüberlegungen: Begehrt der Schädiger wegen unrechtmäßiger Verarbeitung personenbezogener Daten die Löschung des Videos (Art 17 Abs 1 lit e), könnte sich der Geschädigte einerseits mit guten Gründen auf die Notwendigkeit zur Geltendmachung von Rechtsansprüchen berufen (Art 17 Abs 3 lit e).[65]) Sonst wäre es – andererseits – auch nur ein kleiner Schritt zur Haftung des Unfallopfers für einen vorgebrachten immateriellen Schaden des Unfalllenkers, den die unrechtmäßige Datenverarbeitung emotional belastet (Art 82), was unter Gesichtspunkten des Rechtswidrigkeitszusammenhangs aber offenkundig nicht überzeugte.[66]) Die Sanktionierung der Rechtswidrigkeit gegenüber allen anderen Verkehrsteilnehmern sollte insofern nicht in einer Privilegierung des Schädigers als einziger Person liegen, gegenüber der die Aufzeichnung unproblematisch ist. Mit dem BGH müssen die drohenden Verwaltungsstrafen – sowie allfällige Nachteile gegenüber Dritten – vielmehr genügen.[67])

2. Überlange Speicherung

In einer anderen Schattierung gilt das auch für die bereits erwähnte Trafik-Entscheidung des BAG.[68]) Dort war die offene Videoüberwachung zwar erlaubt, allerdings wurden die Aufzeichnungen erst Monate nach den fraglichen Vorfällen

62) Jüngst *Knyrim*, Anm zu VwGH Ro 2020/04/0008, ZVR 2023, 205 mwN.
63) BGH NJW 2018, 2883 Rz 25 f.
64) Rz 39 ff, 43 ff; jüngst auch OLG Saarbrücken NJW 2023, 1065.
65) Zur Handhabung durch die DSB *Haidinger* in *Knyrim*, DatKomm Art 17 DSGVO Rz 74. Alternativ könnte man von vornherein annehmen, dass die Verarbeitung der personenbezogenen Daten des Schädigers gerade nicht rechtswidrig war. Vgl auch EuGH 4. 5. 2023, C-60/22, *Bundesrepublik Deutschland* Rz 48 ff: kein Löschungsanspruch bei Verstößen gegen die Art 26 und 30.
66) Siehe *Werderitsch*, RdW 2021, 242 (245) für jede Verwertung, die den Prozessstandpunkt des Beweisführers stützen kann.
67) BGH NJW 2018, 2883 Rz 52 f.
68) Siehe oben III.A.

gesichtet, als Unregelmäßigkeiten aufgefallen waren. Datenschutzrechtlich ist eine derart lange Speicherung umstritten, wobei das BAG primär von der Zulässigkeit ausging. Es sicherte sich aber zusätzlich ab: Selbst wenn die Videos schon früher zu löschen gewesen wären, könnte man sie im Kündigungsprozess gegen die untreue Verkaufsangestellte verwerten.[69])

Ausschlaggebend war wiederum eine Abwägung der betroffenen Interessen unter überzeugender Berücksichtigung des Schutzzwecks der verletzten Norm. Missbilligt war ja nicht die Aufnahme an sich, sondern deren lange Verfügbarkeit für die Arbeitgeberin. Dabei könnte das Interesse der vorsätzlich schädigenden Verkäuferin am Unterbleiben der überlangen Speicherung für das BAG nur überwiegen, wenn der *„Gefahr einer Verbreitung der Aufzeichnungen zu anderen, die Aufzeichnung nicht rechtfertigenden Zwecken begegnet werden muss."* Im Zivilprozess über ihre Verfehlungen ist das nicht der Fall, vielmehr ist die Videoüberwachung auf genau diese Situation ausgerichtet und hierfür erlaubt. Nun soll durch ein allfälliges Speicherverbot aber *„nicht die Zweckerreichung verhindert, sondern allein eine Zweckentfremdung vereitelt werden"*, zumal auch Aspekte der Generalprävention *„zumindest im Fall einer offenen Überwachung"* kein anderes Ergebnis bedingen.[70])

3. Chat-Protokolle

Insgesamt kristallisiert sich damit ein wesentlicher Wertungsgesichtspunkt heraus. Datenschutz ist Persönlichkeitsschutz (Art 8 GRC), weshalb die Sensibilität mit der Tiefe des Eingriffs in die Privatsphäre wächst. Umgekehrt sinkt das Bedürfnis nach Verwertungsverboten, wenn man die eigenen Daten freiwillig nach außen trägt: Wer per Dashcam gefilmt wird, bewegt sich bewusst in der Öffentlichkeit und kann sich daher nur bedingt über eine *„invasion of privacy"*[71]) beklagen; wer im offen videoüberwachten Raum Gelder abzweigt, tappt in keine Falle, sondern fordert sein Glück heraus.

Dass der Gedanke eines Verlassens der Privatsphäre durchaus weit reicht, belegen „durchgesickerte" Chat-Nachrichten, die in Deutschland offenbar vermehrt bei Arbeitsgerichten aufschlagen. Eine gemeinnützig tätige Einrichtung kündigte etwa einen Mitarbeiter, nachdem sie durch ein anderes Gruppenmitglied das Protokoll einer privaten WhatsApp-Gruppe mehrerer Kollegen erhalten hatte. Daraus ergab sich dessen fremdenfeindliche Gesinnung, was insofern keine reine Privatsache war, als der Arbeitnehmer unter anderem das Qualitätsmanagement im Bereich Migration/Asyl verantwortet hatte. Das LAG Berlin-Brandenburg ließ das Beweismittel zu: Zwar greife die – freilich nicht vom Beweisführer selbst ausgehende[72]) – Offenlegung möglicherweise in das Recht auf informationelle Selbstbestimmung ein; der Betroffene sei allerdings *„nicht ausspioniert"* worden, vielmehr beteiligte er sich bewusst an einem Chat mit bestimmten Personen. *„Wenn*

69) BAG NZA 2018, 1329 Rz 35; demgegenüber zum Beweis von Arbeitszeitbetrug durch unzulässige Videoüberwachungen des Betriebseingangs LAG Niedersachsen BeckRS 2022, 26604; BeckRS 2022, 26626.

70) BAG NZA 2018, 1329 Rz 35.

71) *Bell v. American Traffic Solutions*, 371 F. App'x 488 (5th Cir. 2010): kein Verwertungsverbot bei Verkehrsüberwachung durch ein Unternehmen, das nicht über die erforderliche Lizenz verfügte; dazu *Kodek* in FS Kaissis 523 (530 f).

72) Auf diesen Aspekt weist auch *Rebhahn* in *WiR*, Geheimnisschutz 1 (30) hin.

diese dann seinen Erwartungen der Vertraulichkeit nicht entsprechen, liegt dies mit in seinem Risikobereich."[73])

Aus österreichischer Sicht erinnert diese Überlegung an genuin prozessuale Grundsätze, die vor allem *Kodek* herausgestrichen hat. Vertraut man sich anderen Personen an, nimmt man schließlich einerseits ganz allgemein eine mögliche Zeugenaussage in Kauf, die nach nationalem Verständnis – im Unterschied zu § 383 Abs 3 dZPO – selbst im Fall des Verstoßes gegen eine Verschwiegenheitspflicht verwertbar ist (§ 321 ZPO).[74]) Andererseits sind schriftliche Korrespondenz sowie Film- oder Tonbandaufnahmen von Gesprächen oder sonstigen Kontakten insofern nie völlig abgeschirmt, als im Prozess eine unbedingte Pflicht zur Vorlage der Urkunde oder des Augenscheinsgegenstands[75]) wegen Gemeinschaftlichkeit besteht (§ 304 Abs 1 Z 3, §§ 308, 369 ZPO).[76]) Diese Pflicht rechtfertigt sich wiederum gerade daraus, dass man nicht mit dem Verbleib in der *„prozessfreien Individualsphäre"* rechnen durfte,[77]) womit sich der Kreis schließt.

C. Mögliche Verwertungsverbote

Mit der Wertung einer prozessfreien Individualsphäre schließt sich der Kreis allerdings auch insofern, als sie zu jenen Fällen führt, in denen Verwertungsverbote ernsthaft erwogen werden sollten. Hat man die eigenen Daten nicht nach außen getragen, entfällt ja die angesprochene Rechtfertigung ihrer Verwendung im Prozess. Gleichzeitig wird dieses erhöhte Schutzbedürfnis des Betroffenen regelmäßig mit einem gesteigert missbilligten Verhalten des Beweisführers korrespondieren, der irgendwie – *Ahrens* spricht von *„Schlüssellochtechnik"*[78]) – an die eigentlich privat gehaltenen Daten gelangt ist. Seine strenge Haftung für immaterielle Schäden aus dem „Datenabfluss" sorgt nunmehr zwar immerhin für einen gewissen Ausgleich (Art 82), kuriert aber nur Symptome und beseitigt weder das Unrecht noch seine Folgen.[79]) In solchen Fällen trifft *Rebhahns* zum alten Datenschutzrecht formulierter Befund, effektiver Individualschutz lasse sich neben Strafen nur durch Beweisverwertungsverbote bewerkstelligen, daher nach wie vor zu.[80])

Dabei muss man gar nicht erst auf hoffentlich dystopische Big-Brother-Szenarien wie systematisch lauschende Sprachassistenten oder unbemerkt mitschneidende Webcams zurückgreifen. Vielmehr liefert insb die arbeitsrechtliche Judikatur strukturell ganz ähnlich gelagerte Beispiele: So setzte ein Arbeitgeber etwa ohne berücksichtigungswürdigen Anlass einen verdeckten „Software-Key-

73) LAG Berlin-Brandenburg MMR 2022, 319 Rz 50; ebenso LAG Hannover MMR 2023, 313 Rz 81.

74) *Kodek* in FS Kaissis 523 (535 ff, 544 f). Ergibt sich die Verschwiegenheitspflicht aus der DSGVO (vgl *Spitzer* in *Spitzer/Wilfinger,* Beweisrecht § 321 ZPO Rz 53), muss sich diese Rechtsfolge freilich am europäischen Maßstab bewähren.

75) Dritte sind zwar nicht zur inzidenten Mitwirkung am Augenscheinsbeweis verpflichtet, können bei Gemeinschaftlichkeit aber klageweise zur Vorlage angehalten werden (Art XLIII EGZPO); vgl *Bienert-Nießl*, Materiellrechtliche Auskunftspflichten im Zivilprozess (2003) 140 f.

76) *Kodek*, ÖJZ 2001, 281 (292 f); *Schweiger/Werderitsch*, Zak 2018, 187 (190).

77) *Riss*, Die Gemeinschaftlichkeit der Beweismittel (2016) 185 ff, 193 ff, 196 ff.

78) *Ahrens*, NJW 2018, 2837 (2838).

79) Auf drohende Wertungswidersprüche weist in diesem Zusammenhang *Schild* in BeckOK DatenSR[42] Syst E Rz 40a hin.

80) *Rebhahn*, Mitarbeiterkontrolle 28 f; s auch *L. Schmid*, ÖJZ 2018, 75 (75).

logger" ein, um unbemerkt alle Tastatureingaben am Dienst-PC zu erfassen und regelmäßig Screenshots zu fertigen;[81]) nachlassende Produktivität im Homeoffice bescherte einem Vertriebsleiter eine detektivische Observation gleichsam durch das Wohnzimmerfenster;[82]) ein Arbeitgeber suchte auf dem Diensthandy nach Anhaltspunkten für Verfehlungen und wertete gleich auch *„Tausende"* private Bilder und Videos aus.[83]) Jeweils wurden also Daten tief aus der Sphäre des Betroffenen erlangt, der damit nicht rechnen musste, sondern berechtigterweise davon ausgehen durfte, sich *„ins Unreine"*[84]) verhalten zu können. In Österreich ließe sich denn auch weder auf die Inkaufnahme von Zeugenaussagen noch auf eine unbedingte Mitwirkungspflicht (§ 305 ZPO) rekurrieren,[85]) weil der Betroffene seine prozessfreie Individualsphäre nie verließ.[86]) Während es hierzulande wohl trotzdem zur Verwertung gekommen wäre, zogen die befassten deutschen Gerichte die Konsequenzen. Sie lehnten die Berücksichtigung der so erlangten Informationen und Beweismittel durchgehend ab.[87])

Die DSGVO könnte dieses Ergebnis nun zum europäischen Standard machen.[88]) Auch im Rahmen des Beweisverfahrens dürfen personenbezogene Daten eben nur verarbeitet werden, soweit es der Justizgewährungsanspruch verlangt,[89]) wobei die Feinprüfung in eine Interessenabwägung mündet.[90]) Steht die Erforderlichkeit der Datenverarbeitung „zur Wahrung der berechtigten Interessen des Verantwortlichen" der Erforderlichkeit des Datenschutzes zur Wahrung der „Interes-

81) BAG NZA 2017, 1327 Rz 20. Konkret war den Arbeitnehmern zwar angekündigt worden, dass es Kontrollen gibt; dass es sich um eine lückenlose Überwachung handelte, war aber nicht bekannt; vgl auch *Niemann*, Jb Arbeitsrecht 55 (2018) 41 (56). *Stella/Winter*, ZAS 2020, 252 (256) weisen auf eine ganz ähnliche Entscheidung des Schweizerischen Bundesgerichts hin.

82) LAG Berlin-Brandenburg ZD 2021, 170.

83) ArbG Mannheim BeckRS 2021, 42451. Im Einzelnen müsste man freilich fragen, welche Informationen nun genau verwertet werden sollten, weil zwischen privaten Videos und beruflichen Nachrichten ein Unterschied besteht. Außerdem liegt der Fall insofern speziell, als dem Arbeitnehmer die Löschung der privaten Daten vor der Retournierung des Telefons misslungen war und er die Daten daher – wenn auch versehentlich – selbst aus der Hand gab.

84) Siehe hierzu *Kodek*, ÖJZ 2001, 281 (295); *Riss*, Gemeinschaftlichkeit 187. BVerfG und BGH führen diesen Aspekt sogar mit Blick auf Lauschzeugen ins Treffen, die ein Gespräch unbemerkt mithören (BVerfG NJW 2002, 3619; BGH JZ 2003, 1109), obwohl der Betroffene hier weniger schutzwürdig ist. Ihm war ja zumindest bewusst, dass seine Aussagen dem Gesprächspartner zur Kenntnis gelangen; vgl *Foerste*, JZ 2003, 1111 (1112); *Kodek* in FS Kaissis 523 (545).

85) Im Diensthandy-Fall lag es freilich am Versehen des Betroffenen, dass der Gegner das Beweismittel erlangte.

86) Für einen Gleichlauf der Verwertungsmöglichkeit *Dilcher*, Die prozessuale Verwendungsbefugnis, AcP 158 (1959/1960) 469 (475 ff); dagegen *Kodek* in FS Kaissis 523 (542).

87) Dabei wird in Deutschland sogar von einem entsprechenden „Sachvortragsverwertungsverbot" ausgegangen, um den Betroffenen vor dem Hintergrund der weitgehenden Geständnisfiktion des § 138 Abs 3 dZPO nicht zur Säumnis oder Lüge zu zwingen; näher *Niemann*, Jb Arbeitsrecht 55 (2018) 41 (44, 63 ff); krit *Thole* in *Stein/Jonas*, ZPO[23] § 286 Rz 56.

88) So auch *Stella/Winter*, ZAS 2020, 252 (256).

89) Den Größenschluss aus Art 9 Abs 2 lit f (s oben II.A.) zieht der EuGH schon bei rechtmäßig erlangten Daten nicht. Außerdem erscheint zweifelhaft, ob die Verarbeitung unrechtmäßig erlangter Daten überhaupt mitgemeint ist; dafür *Werderitsch*, EF-Z 2022, 286 (287).

90) Siehe oben II.B.

sen oder Grundrechte […] der betroffenen Person" gegenüber (Art 6 Abs 1 lit f),[91]) lässt sich eine Prognose zur Haltung des EuGH wagen: Die Zulässigkeit der prozessualen Verarbeitung von Daten, die der Beweisführer etwa durch versteckte Keylogger, heimliche Aufnahmen oder übergriffige Auswertungen erhoben hat, würde genauso überraschen wie die Versagung des Löschungsanspruchs wegen Erforderlichkeit solcher Daten zur Rechtsdurchsetzung (Art 17 Abs 3 lit e).

Im Einzelfall können sich daran zwar wiederum Folgefragen etwa nach Gesichtspunkten wie besonderer Beweisnot oder der Abwehr von Prozessbetrug knüpfen.[92]) Jedenfalls dürfte hier aber ein Einfallstor für datenschutzrechtliche Beweisaufnahme- und -verwertungsverbote per Interessenabwägung liegen. Während sich das deutsche Abwägungsmodell vor diesem Hintergrund bereits *„wunderbar"* in das Normgefüge der DSGVO einfügen mag,[93]) muss Österreich dementsprechend nachziehen. Verwertungsverbote stehen nunmehr wirklich im Raum.

IV. Schluss

Ganz verschont bleibt das Beweisrecht also nicht. Schon der kleine Ausschnitt hat allerdings gezeigt, wie weit die angesprochenen Fälle auseinanderliegen. Rechtmäßig erhobene sind von rechtswidrig erlangten Daten zu unterscheiden und auch innerhalb dieser Gruppe ist zu differenzieren, weil sich der Verstoß gegenüber dem Betroffenen manchmal gar nicht, mitunter aber erheblich auswirkt.

Aus österreichischer Sicht gibt es jedenfalls auch unter der DSGVO keinen Grund zur Sorge vor überhandnehmenden Einschränkungen der gerichtlichen Wahrheitserforschung durch einen hochstilisierten Datenschutz, wobei der EuGH mit klaren Fällen natürlich nicht befasst werden muss. Begründete Zweifel bestehen aber daran, ob sich die verbreitete kategorische Ablehnung von Verwertungsverboten aufrechterhalten lässt. Spätestens bei tiefgreifenden Verletzungen der Privatsphäre müsste eine Interessenabwägung nämlich oft zu Gunsten des Betroffenen ausgehen.

---

91) Näher *Kastelitz/Hötzendorfer/Tschohl* in *Knyrim,* DatKomm Art 6 DSGVO Rz 51 ff. EuGH 4. 5. 2023, C-60/22, *Bundesrepublik Deutschland* Rz 73, wonach die Datenverarbeitung durch Gerichte nach Art 6 Abs 1 lit e erforderlich sei, lässt sich auf die hier interessierenden Fälle nicht übertragen. In der Entscheidung ging es nämlich nicht um Beweismittel, sondern um die Aktenführung selbst (Rz 29), die gegenüber dem Betroffenen außerdem gar keine rechtswidrige Verarbeitung darstellte (Rz 61, 74).

92) Zu den damit verbundenen Schwierigkeiten etwa *Kodek* in FS Kaissis 523 (546 f); *Kodek*, ecolex 2022, 977 (977); *Foerste*, Lauschzeugen im Zivilprozess, NJW 2004, 262.

93) *Waldkirch*, VersR 2020, 1141 (1155).